Nations Unies

S/PV.7882



Conseil de sécurité

Soixante-douzième année

Provisoire

7882e séance

Lundi 13 février 2017, à 10 heures

New York

Président :	M. Klimkin/M. Vitrenko	(Ukraine)
Membres :	Bolivie (État plurinational de)	M. Arancibia Fernández
	Chine	M. Liu Jieyi
	Égypte	M. Aboulatta
	États-Unis d'Amérique	M. Klein
	Éthiopie	M. Alemu
	Fédération de Russie	M. Zagaynov
	France	M. Lamek
	Italie	M. Amendola
	Japon	M. Bessho
	Kazakhstan	M. Abdymomunov
	Royaume-Uni de Grande-Bretagne et d'Irlande du Nord	M. Rycroft
	Sénégal	M. Seck
	Suède	M. Skoog
	Uruguay	M. Bermúdez

Ordre du jour

Menaces contre la paix et la sécurité internationales résultant d'actes de terrorisme

Protection des infrastructures essentielles contre les attaques terroristes

Lettre datée du 1er février 2017, adressée au Secrétaire général par le Représentant permanent de l'Ukraine auprès de l'Organisation des Nations Unies (S/2017/104)

17-03824 (F)





La séance est ouverte à 10 h 10.

Adoption de l’ordre du jour

L’ordre du jour est adopté.

Menaces contre la paix et la sécurité internationales résultant d’actes de terrorisme

Protection des infrastructures essentielles contre les attaques terroristes

Lettre datée du 1er février 2017, adressée au Secrétaire général par le Représentant permanent de l’Ukraine auprès de l’Organisation des Nations Unies (S/2017/104)

Le Président (*parle en anglais*) : Conformément à l’article 37 du règlement intérieur provisoire du Conseil, j’invite les représentants de l’Afghanistan, de l’Afrique du Sud, de l’Albanie, de l’Algérie, de l’Allemagne, de l’Argentine, de l’Australie, de l’Autriche, du Bangladesh, de la Belgique, du Brésil, de la Bulgarie, du Canada, du Chili, de la Colombie, de la Croatie, de Cuba, du Danemark, des Émirats arabes unis, de l’Espagne, de l’Estonie, de l’ex-République yougoslave de Macédoine, de la Finlande, de la Géorgie, de la Grèce, d’Haïti, de l’Inde, de l’Indonésie, de l’Iraq, de l’Islande, d’Israël, de la Jordanie, du Koweït, de la Lettonie, du Luxembourg, de la Malaisie, des Maldives, de Malte, du Maroc, du Monténégro, de la Nouvelle-Zélande, du Pakistan, des Pays-Bas, du Pérou, de la Pologne, de la République arabe syrienne, de la République bolivarienne du Venezuela, de la République de Corée, de la République de Moldova, de la République islamique d’Iran, de la République tchèque, de la Roumanie, de la Slovaquie, Slovénie et de la Turquie à participer à la présente séance.

Conformément à l’article 39 du règlement intérieur provisoire du Conseil, j’invite les personnalités suivantes appelées à faire un exposé à participer à la présente séance : Mme Maria Luiza Ribeiro Viotti, Directrice de cabinet du Secrétaire général; M. Jürgen Stock, Secrétaire général de l’Organisation internationale de police criminelle; M. Hamid Ali Rao, Directeur général adjoint de l’Organisation pour l’interdiction des armes chimiques; M. Chris Trelawny, Conseiller spécial du Secrétaire général de l’Organisation maritime internationale, chargé de la sûreté maritime et de la simplification des formalités; et M. Olli Heinonen, Conseiller principal pour les sciences et la non-prolifération à la Foundation for Defense of Democracies et ancien Directeur général adjoint de l’Agence internationale de l’énergie atomique.

M. Stock participe à la présente séance par visioconférence depuis Lyon.

Conformément à l’article 39 du règlement intérieur provisoire du Conseil, j’invite également les personnes suivantes à participer à la présente séance : M. João Vale de Almeida, Chef de la délégation de l’Union européenne auprès de l’Organisation des Nations Unies, et M. Krisztian Meszaros, Officier de liaison civil de l’Organisation du Traité de l’Atlantique Nord auprès de l’ONU.

Je propose que le Conseil invite l’Observateur permanent de l’État observateur du Saint-Siège auprès de l’Organisation des Nations Unies à participer à la séance, conformément au règlement intérieur provisoire et à la pratique établie,.

Puisqu’il n’y a pas d’objection, il en est ainsi décidé.

Le Conseil de sécurité va maintenant aborder l’examen de la question inscrite à son ordre du jour.

J’appelle l’attention des membres du Conseil sur le document S/2017/104, qui contient le texte d’une lettre datée du 1er février 2017, adressée au Secrétaire général par le Représentant permanent de l’Ukraine auprès de l’Organisation des Nations Unies, transmettant une note de cadrage relative à la question à l’examen.

Les membres du Conseil sont saisis du document S/2017/119, qui contient le texte d’un projet de résolution déposé par l’Albanie, l’Allemagne, l’Autriche, la Belgique, la Bulgarie, le Canada, le Chili, la Croatie, le Danemark, les Émirats arabes unis, l’Espagne, l’Estonie, les États-Unis d’Amérique, l’ex-République yougoslave de Macédoine, la Finlande, la France, la Géorgie, la Grèce, l’Iraq, l’Islande, Israël, l’Italie, le Japon, la Lettonie, le Luxembourg, la Malaisie, Malte, le Monténégro, la Nouvelle-Zélande, les Pays-Bas, la Pologne, la République de Moldova, la République tchèque, la Roumanie, le Royaume-Uni de Grande-Bretagne et d’Irlande du Nord, la Slovaquie, la Slovénie, la Suède, la Turquie, l’Ukraine et l’Uruguay.

Le Conseil est prêt à voter sur le projet de résolution dont il est saisi. Je vais maintenant mettre aux voix le projet de résolution.

Il est procédé au vote à main levée.

Votent pour :

Bolivie (État plurinational de), Chine, Égypte, Éthiopie, France, Italie, Japon, Kazakhstan, Fédération de Russie, Sénégal, Suède, Ukraine, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, États-Unis d'Amérique, Uruguay

Le Président (*parle en anglais*) : Le résultat du vote est le suivant : 15 voix pour. Le projet de résolution est adopté à l'unanimité en tant que résolution 2341 (2017).

Le 21 novembre 2016, le Conseil de sécurité a tenu une réunion selon la formule Arria sur la protection des infrastructures essentielles contre les attaques terroristes. Cette réunion a démontré la compréhension croissante par les États Membres de l'ONU de l'importance du sujet et a mis en lumière l'urgente nécessité de maintenir un niveau élevé de protection des infrastructures essentielles et de consolider les efforts faits au niveau international pour accroître leur résilience face aux attaques terroristes. La résolution qui vient d'être adoptée est, à notre avis, une réponse opportune de la communauté internationale face aux menaces nouvelles et en évolution rapide posées par le terrorisme. Il s'agit d'une mesure décisive de préparation mondiale aux attentats terroristes contre les infrastructures essentielles et pour le renforcement de la coopération internationale en la matière. J'encourage les participants au débat d'aujourd'hui à présenter de manière détaillée leurs priorités et les difficultés rencontrées, à fournir des informations sur leurs efforts actuels et à partager les bonnes pratiques en matière de protection des infrastructures essentielles.

Je donne maintenant la parole à Mme Viotti.

Mme Viotti (*parle en anglais*) : C'est un plaisir de me trouver ici aujourd'hui pour représenter le Secrétaire général. Je tiens à vous féliciter, Monsieur le Président, d'avoir convoqué la présente séance.

Comme les organisations terroristes prolifèrent et cherchent de nouveaux moyens de planifier et d'exécuter des attaques matérielles et des cyberattaques dans le monde entier, la menace qu'elles posent devient de plus en plus complexe. Les infrastructures essentielles sont particulièrement vulnérables, notamment les installations et réseaux énergétiques; les transports aériens, terrestres et maritimes; les services bancaires et financiers; l'approvisionnement en eau; la distribution alimentaire, la santé publique et les autres services indispensables à toute société moderne. Les réseaux et systèmes infrastructurels qui auparavant fonctionnaient indépendamment sont désormais interconnectés du fait des progrès de la technologie des communications et de l'information. Une attaque dirigée contre un secteur peut en affecter d'autres, conduisant à des perturbations et à un chaos général.

La Direction exécutive du Comité contre le terrorisme a reconnu la gravité des dangers que font courir Daech et d'autres groupes déterminés à conduire de telles attaques. En outre, puisque beaucoup de ces installations et réseaux ont un champ d'opérations transfrontalier, toute attaque terroriste contre eux aurait presque certainement des implications régionales et mondiales. Le caractère transnational du terrorisme exige une réaction coordonnée de la part de tous les États et de tous les acteurs de la communauté internationale.

Il nous faut pourtant admettre que la coopération internationale contre le terrorisme a été limitée, surtout dans le domaine des infrastructures essentielles. Sur le plan stratégique, cela signifie que la communauté internationale doit s'unir et se montrer plus créative, active et efficace, notamment avec la création de solides partenariats public-privé. Il faut prendre trois mesures clefs.

Premièrement, il faut dresser la carte des vulnérabilités des infrastructures essentielles à tous les niveaux et dans tous les secteurs. Deuxièmement, les acteurs internationaux, régionaux et nationaux doivent coopérer en matière de prévention et, en cas d'attaque, en matière d'atténuation de ses effets, notamment par le partage de l'information. Troisièmement, il est capital de renforcer la capacité des États, notamment s'agissant d'évaluer les risques, de prendre des mesures de préparation aux situations d'urgence, de renforcer la capacité de gestion de ces situations et de veiller à ce que les réactions respectent pleinement les normes régissant les droits de l'homme. L'ONU se tient prête à assister les États Membres dans ces domaines et dans d'autres.

L'Équipe spéciale chargée de mettre en œuvre la lutte contre le terrorisme a créé le Groupe de travail interorganisations pour la protection des infrastructures essentielles, entre autres Internet, Cibles vulnérables et Sécurité du tourisme. Divers projets visant à assister les États Membres sont en cours; ils embrassent de nombreux domaines, entités et partenaires des Nations Unies. Mais, bien entendu, la responsabilité première appartient aux États Membres.

Le présent débat se situe à un moment crucial. Comme notre monde est de plus en plus interconnecté

par les voyages, le commerce et les communications, comme aussi dans le cyberespace, nous devenons plus vulnérables aux attaques de terroristes experts en technologie qui cherchent de nouveaux moyens de répandre la crainte. Il est encourageant que le Conseil de sécurité porte une attention accrue à cette menace critique.

Le Président (*parle en anglais*) : Je remercie Mme Viotti de son exposé.

Je donne maintenant la parole à M. Stock.

M. Stock (*parle en anglais*) : C’est un honneur de prononcer de nouveau un exposé devant le Conseil de sécurité, et sur une question d’importance capitale pour notre sécurité collective.

Je tiens à remercier l’Ukraine d’avoir convoqué cette séance et de ses efforts continus pour mobiliser la coopération internationale sur ce sujet crucial.

Les infrastructures essentielles font fonction de système indispensable à l’existence quotidienne. Nos sociétés reposent sur un réseau fort complexe et perfectionné de systèmes infrastructurels. Les citoyens s’en remettent à des institutions et services en bon état de fonctionnement pour leur santé, leur sécurité et leur bien-être économique. Ce système indispensable à la vie est devenu plus efficient et productif grâce aux progrès technologiques, aux échanges liés à la mondialisation et aux exigences d’une population de plus en plus urbanisée. L’avènement de « life 3.0 » – le chevauchement des mondes numérique et physique – noua a permis de surveiller, même de contrôler, l’infrastructure depuis n’importe quel point du monde.

Cependant, du fait de cette extrême dépendance et de la connectivité, nous sommes devenus vulnérables aux menaces. L’interdépendance de notre infrastructure à travers les secteurs et les industries, entre les domaines informatique et physique, et au-delà des frontières nationales, signifie que les conséquences d’une attaque porteraient loin. Une attaque sur un seul point pourrait conduire à la perturbation ou la destruction de multiples systèmes vitaux dans le pays directement touché, et avoir des retombées au niveau mondial. Cela constitue une cible attirante pour ceux qui veulent nous nuire et, à mesure que nos villes et notre infrastructure évoluent, leurs armes évoluent aussi. Les tactiques suivies dans les zones de conflit – par exemple, action simultanée de divers tireurs, engins explosifs improvisés à bord de véhicules blindés, vestes d’explosifs, piratages informatiques ou mini-drones chargés d’explosifs – pourraient être adaptées pour servir dans les rues de nos villes et contre nos installations clefs.

Alors comment pouvons-nous protéger notre système indispensable à la vie contre cette menace en permanente mutation? En un mot, nous le pouvons en rendant tous les acteurs pertinents capables de se préparer à de telles attaques, de les prévenir et d’y répondre. Ces impératifs se situent au cœur des efforts d’INTERPOL et de nos partenaires du Groupe de travail inter-organisations pour la protection des infrastructures essentielles, entre autres Internet, Cibles vulnérables et Sécurité du tourisme, qui relève de l’Équipe spéciale chargée de mettre en œuvre la lutte contre le terrorisme, visant à promouvoir le partage du renseignement, le renforcement des capacités et la résilience dans certains domaines cruciaux.

Premièrement, nous mettons l’accent sur le renforcement de la sécurité des sites critiques au moyen de normes et procédures de préparation aux situations d’urgence. Par exemple, l’Équipe des cibles vulnérables d’INTERPOL a travaillé avec nos pays membres, en Afrique de l’Ouest, à améliorer la sécurité des laboratoires contenant de dangereux agents pathogènes et à les protéger contre les attaques terroristes. Avec le financement généreux du Gouvernement canadien, ce projet vise à édifier des plans d’action pour la biosécurité au moyen d’une initiative conjointe inter-organisations.

Deuxièmement, nous continuons à exhorter les pays à protéger leurs frontières et à freiner la mobilité des terroristes. Comme il est indiqué dans le rapport du Secrétaire général sur la menace posée par l’État islamique d’Iraq et du Levant (S/2017/97), examiné ici la semaine dernière (voir S/PV/7877), d’octobre 2016 à janvier 2017 INTERPOL a observé une augmentation de 63 % du nombre de profils de combattants terroristes étrangers accessibles à travers son système d’information, et une augmentation de 750 % du partage de l’information entre les pays membres à travers ses propres circuits. C’est là un fait sans précédent dans un domaine aussi sensible; l’appel lancé par le Conseil de sécurité a radicalement changé la situation.

Troisièmement, il est essentiel de rester vigilants et d’intensifier les efforts pour interdire matériaux et outils avant qu’ils ne servent à produire la prochaine arme. Dans ce contexte, INTERPOL agit en liaison étroite avec l’Agence internationale de l’énergie atomique s’agissant de limiter le trafic illicite des matériaux radiologiques et nucléaires en formant à la

surveillance et à la détection et au moyen d'opérations transfrontières.

Enfin et surtout tout, INTERPOL encourage la collaboration inter-organisations et internationale en tant qu'elle a pour effet de multiplier les forces. Il est capital d'échanger les informations, de déceler les menaces immédiates et de suivre les meilleures pratiques aux fins d'identifier les vulnérabilités, les méthodologies et les enseignements tirés.

Dans le domaine du maintien de l'ordre, nous avons nettement conscience de ce paradoxe tragique : un incident terroriste est souvent l'occasion d'apprendre et d'améliorer. Communiquer ces enseignements au-delà des frontières, c'est recueillir des avantages sans avoir à en payer le coût. Tout le monde y gagne. Ensemble, nous pouvons créer un dispositif mondial de sécurité des infrastructures et des mécanismes d'intervention en cas d'incident sur la base d'expériences opérationnelles réelles. Parallèlement, nous pouvons nous mettre à l'épreuve sur des scénarios crédibles auxquels nous pourrions être confrontés à l'avenir.

À cette fin, INTERPOL organise des rencontres à l'intention d'experts qui représentent toutes les parties concernées. Le colloque conjoint organisé en collaboration avec le FBI en est un bon exemple. Le problème de sécurité informatique, que nous avons récemment conçu avec le concours de spécialistes du secteur privé, est un autre exemple de la manière dont nous collaborons avec les pays membres et les donateurs pour nous préparer aux menaces, les prévenir et les combattre, qu'elles soient physiques, informatiques ou portent sur les deux plans.

Dans un monde interconnecté, nous ne parviendrons pas à protéger nos infrastructures nationales dans l'isolement. C'est pourquoi des initiatives telles que la présente séance, et les mesures que prendra par la suite la communauté internationale, sont essentielles.

Le Président (*parle en anglais*) : Je remercie M. Stock de son exposé.

Je donne maintenant la parole à M. Rao.

M. Rao (*parle en anglais*) : Je tiens tout d'abord à vous féliciter, Monsieur le Président, de votre accession à la présidence du Conseil de sécurité. Au nom du Directeur général de l'Organisation pour l'interdiction des armes chimiques (OIAC), je vous remercie d'avoir invité l'OIAC à présenter un exposé sur cette question importante.

Cette année, l'OIAC célèbre 20 ans de collaboration en vue de débarrasser le monde des armes chimiques. Alors que nous sommes en bonne voie s'agissant d'éliminer de manière vérifiable toutes les armes chimiques déclarées par les États détenteurs d'ici le début de la prochaine décennie, nous redoublons d'efforts pour prévenir leur réapparition.

L'OIAC n'est pas une organisation de lutte contre le terrorisme, mais il convient de rendre hommage à l'engagement de ses États parties, qui reconnaissent en elle une instance capable d'apporter une contribution significative à la lutte mondiale contre le terrorisme, en particulier en ce qui concerne la menace du terrorisme chimique.

Depuis 2009, l'OIAC met en œuvre et développe des programmes de coopération internationale dont l'objectif est de renforcer la sécurité chimique mondiale. À la demande des États parties, l'OIAC procède à une évaluation globale des risques pour les aider à déterminer les menaces à la sécurité chimique. L'objectif du renforcement des capacités dans ces pays est de contribuer à l'évaluation des risques, au renforcement de la vigilance, à la mise en place de mesures de protection et à la réaction aux menaces. Les programmes de renforcement des capacités font intervenir un grand nombre d'acteurs, notamment les responsables de la gestion des installations, la police, les universitaires, le personnel des laboratoires et les experts en défense nucléaire, radiologique, biologique et chimique, et ce en vue de renforcer le cadre de sécurité au niveau national. Des experts originaires de pays voisins participent, le cas échéant, aux efforts visant à consolider l'implantation du cadre de sécurité au niveau régional.

Alors que nous sommes en train de renforcer notre rôle en tant que plateforme d'échange d'informations et de coordination, nous avons donné un nouvel élan aux activités du Groupe de travail à composition non limitée sur le terrorisme en créant un sous-groupe de travail qui se penche sur la question des acteurs non étatiques. Le Groupe examine les aspects juridique et relatifs à la prévention et aux interventions contre le terrorisme chimique. Le secrétariat de l'OIAC a également renforcé sa capacité à aider les États parties à réagir à d'éventuels actes de terrorisme chimique. Une mission d'assistance et d'intervention rapides a été créée au siège de l'OIAC et peut être déployée rapidement dans tout État partie touché par un incident chimique impliquant l'emploi

présumé de produits chimiques toxiques par un acteur non étatique. La mission ne sera déployée qu’à la demande de l’État partie touché. L’équipe sera dotée des moyens nécessaires pour sécuriser la zone touchée, détecter les matières chimiques toxiques et fournir des conseils en matière de décontamination et d’assistance immédiate aux victimes. Concrètement, l’équipe aura les moyens d’agir en coopération et en coordination avec l’ONU et les autres organisations internationales compétentes. En janvier, la mission a été testée dans le cadre d’un exercice de simulation organisé parallèlement à une réunion de l’Équipe spéciale de lutte contre le terrorisme au siège de l’OIAC.

Deuxièmement, nous collaborons avec l’industrie chimique. Des centaines de milliers de tonnes de produits chimiques inscrits sont échangées chaque année au niveau international. Alors que l’industrie chimique mondiale continue de se développer en taille et complexité, une priorité importante consiste à garantir que ces produits chimiques ne sont jamais échangés, sciemment ou non, à des fins interdites par la Convention sur les armes chimiques. La sécurité de la chaîne d’approvisionnement en produits chimiques jouera un rôle crucial dans la protection des populations et de l’environnement contre l’utilisation de produits chimiques toxiques à des fins hostiles.

Nous avons vu les terribles conséquences humaines et environnementales que peuvent avoir les accidents chimiques. Les dégâts potentiels ne peuvent que s’aggraver si de tels événements sont volontairement causés par des acteurs qui veulent nuire. La récente attaque qui a visé une usine chimique près de Mossoul, en Iraq, illustre on ne peut plus clairement les risques auxquels nous sommes exposés si ceux qui veulent nuire et semer la terreur visent en priorité les infrastructures chimiques. L’industrie et les gouvernements doivent assumer une part de responsabilité égale si nous voulons renforcer la sécurité chimique face aux attaques terroristes. L’industrie chimique mondiale est pleinement consciente de la nécessité de prévenir toute utilisation abusive des produits chimiques et d’assurer la protection physique des usines chimiques, et nous continuons de renforcer notre collaboration avec l’industrie chimique mondiale.

Troisièmement, nous collaborons avec nos partenaires internationaux. La lutte contre le terrorisme chimique exige de suivre une démarche globale dans le domaine de la sécurité en s’appuyant sur un réseau de parties intéressées et de partenaires internationaux. Nous collaborons avec des organisations internationales influentes par l’intermédiaire de l’Équipe spéciale de lutte contre le terrorisme, un organe qui fait partie de la Stratégie antiterroriste mondiale des Nations Unies. L’Équipe spéciale a pour objectif d’améliorer la préparation et de renforcer la capacité de réaction sur la base d’un cadre commun et cohérent. En tant que Coprésident du Groupe de travail sur la prévention des attentats terroristes à l’arme de destruction massive et les interventions en cas d’attentat, l’OIAC appelle au renforcement de la coordination interinstitutions pour faire face à un acte de terrorisme chimique. Le mois dernier, l’OIAC a organisé un exercice de simulation en collaboration avec le Groupe de travail pour définir clairement les capacités d’intervention et les lacunes en la matière. L’objectif de cet exercice était de créer un vaste système d’action mondiale et de garantir que tout pays qui demande de l’aide la recevra dans le cadre d’une démarche coordonnée et efficace.

En janvier également, l’OIAC a signé un mémorandum d’accord avec l’Organisation mondiale des douanes. Le renforcement de la coopération avec l’Organisation mondiale des douanes est envisagé en vue de renforcer les contrôles nationaux et internationaux appliqués au commerce de produits chimiques toxiques.

Les membres du Conseil sont pleinement conscients des efforts déployés par l’OIAC en collaboration avec l’ONU aux fins d’éliminer le programme d’armes chimiques de la République arabe syrienne. Plus de 30 pays ont promis d’affecter des ressources financières et techniques à cette initiative. Le secteur privé a joué un rôle capital, étant donné que des entreprises chimiques ont participé dans de nombreux pays à l’élimination de certains de ces agents. Bien que des progrès aient été enregistrés, notre travail en Syrie n’est pas terminé. Il est profondément regrettable que des armes chimiques continuent d’être utilisées dans ce pays. En Libye, la menace que posent les acteurs non étatiques a poussé les autorités libyennes à demander de l’aide afin de retirer et de détruire les derniers vestiges de l’ancien programme d’armes chimiques de ce pays. Cette opération se déroule actuellement avec succès grâce à la coopération et l’appui de nos États membres.

Un monde exempt d’armes chimiques ne verra le jour que moyennant une prise de conscience totale, une vision commune et un attachement inlassable à la coopération internationale. La Convention sur les armes chimiques affirme une détermination commune à ne jamais laisser la chimie être utilisée contre l’humanité.

Sur cette base, nous continuerons de collaborer avec toutes les parties intéressées afin de renforcer la capacité mondiale à prévenir et, le cas échéant, détecter et combattre les actes de terrorisme chimique.

Le Président (*parle en anglais*) : Je remercie M. Rao de son exposé.

Je donne maintenant la parole à M. Trelawny.

M. Trelawny (*parle en anglais*) : Le Secrétaire général de l’Organisation maritime internationale (OMI), M. Kitack Lim, remercie le Président du Conseil de sécurité et le Gouvernement ukrainien de l’avoir invité à participer à ce débat public de haut niveau sur la protection des infrastructures essentielles contre les attaques terroristes. Il regrette de ne pas pouvoir être ici en personne, mais m’a demandé de donner lecture de sa déclaration.

L’OMI est une institution spécialisée des Nations Unies chargée de la sûreté, de la sécurité et de l’efficacité des transports maritimes internationaux ainsi que de la protection du milieu marin. Pour ce qui est du cadre juridique relatif à la protection des infrastructures essentielles, l’OMI est l’organisation responsable de la Convention visant à faciliter le trafic maritime international; de la Convention internationale pour la sauvegarde de la vie humaine en mer, y compris le Code international pour la sûreté des navires et des installations portuaires; et des Conventions de 1988 et 2005 pour la répression d’actes illicites contre la sécurité de la navigation maritime et de leurs Protocoles relatifs à la répression d’actes illicites contre la sécurité des plateformes fixes situées sur le plateau continental . Ensemble, ces instruments internationaux constituent un cadre juridique solide qui permet aux Parties de traduire en justice les auteurs d’incidents et qui facilite les activités de l’OMI dans le domaine de la sécurité maritime, notamment sa coopération active avec la Direction exécutive du Comité contre le terrorisme du Conseil de sécurité et l’Équipe spéciale de lutte contre le terrorisme de l’Assemblée générale.

Dans le domaine de la sécurité, l’OMI se concentre sur ce que l’industrie maritime civile – c’est-à-dire les secteurs maritime et portuaire – et le secteur offshore peuvent faire pour se protéger et protéger les autres contre des menaces éventuelles à la sécurité maritime, y compris les actes de terrorisme, et aider les gouvernements à mettre en œuvre de mesures de sécurité adéquates pour protéger le commerce maritime mondial. L’accent est mis sur la sécurité préventive au moyen d’un processus continu de gestion des risques, qui prévoit des procédures de dissuasion et de prévention de menaces, plutôt que des mesures de lutte contre le terrorisme à proprement parler.

Les mesures spéciales visant à renforcer la sécurité maritime, énoncées en détail au chapitre XI-2 de la Convention internationale pour la sauvegarde de la vie humaine en mer et dans le Code international pour la sûreté des navires et des installations portuaires, constituent un cadre pratique fondé sur l’analyse des risques qui concerne non seulement la sécurité maritime mais qui se prête également à une application plus large. S’il est vrai que la Convention traite de la sauvegarde de la vie humaine en mer et par conséquent soulève des problèmes de compétence à terre, où sont appliquées la plupart des mesures préventives de sécurité, pour régler cette question, l’OMI a laissé aux États membres la latitude de définir les limites géographiques de leurs installations portuaires, notamment leur application aux installations offshore. L’OMI a également coopéré avec l’Organisation internationale du Travail (OIT) pour élaborer un Recueil de directives pratiques sur la sûreté dans les ports, qui dans les faits étendent l’application du Code international pour la sûreté des navires et des installations portuaires à la zone portuaire dans son ensemble. En outre, la coopération de l’OMI et de l’Organisation mondiale des douanes en ce qui concerne la sécurité des conteneurs a conduit à l’élaboration et à l’adoption, en juin 2005, du Cadre de normes visant à sécuriser et à faciliter le commerce mondial .

S’agissant de la mise en œuvre pratique du chapitre X1-2 de la Convention internationale et du Code international pour la sûreté des navires et des installations portuaires, on peut dire à juste titre que les problèmes se posent principalement au niveau des installations portuaires. Contrairement aux navires, où il a été relativement facile d’évoluer d’une culture de sûreté à une culture de sécurité, la structure de sécurité dans les ports est généralement beaucoup plus complexe, car elle implique de nombreux acteurs de différentes entités gouvernementales, policières et privées. Pour de nombreux pays, les ports sont des infrastructures essentielles et leur sécurité est une composante de la sécurité nationale. Toutefois, en l’absence de lois, de politiques et d’orientations nationales et locales claires permettant de coordonner les activités de toutes les parties prenantes clefs, les interventions en matière de sécurité dans les ports sont pour le moins fragmentées.

Une stratégie préventive fondée sur l'analyse des risques et bien coordonnée est essentielle pour assurer l'efficacité des régimes de sécurité des ports et des installations portuaires, qu'il s'agisse de protéger les infrastructures portuaires contre les attaques terroristes, de lutter contre le vol et d'autres activités criminelles ou d'empêcher les terroristes, les trafiquants de drogues ou les passagers clandestins d'y avoir accès. Même si l'OMI n'a pas reçu mandat de surveiller le respect par les installations portuaires des normes énoncées au chapitre X1-2 de la Convention et dans le Code international pour la sûreté des navires et des installations portuaires, il est évident que l'absence de comités chargés de la sécurité des ports et des installations portuaires indique qu'il n'y a pas de coopération interinstitutions et que donc la sécurité des installations portuaires n'est pas assurée de manière efficace. La promotion des mécanismes de coordination prévus par le Recueil de directives pratiques publié par l'OIT et l'OMI et par d'autres directives publiées par l'OMI est au cœur de nos efforts visant à promouvoir un respect accru des dispositions du chapitre X1-2 et du Code.

En fait, depuis 2001, l'OMI a mis au point toute une série de directives, d'outils d'auto-évaluation et de matériel didactique pour assurer la protection des ports, des navires et des installations offshore. Il s'agit notamment de cours types destinés aux agents chargés d'assurer la sécurité des installations portuaires; de directives sur la formation et la certification des agents de sûreté des installations portuaires; de directives sur l'auto-évaluation volontaire par les gouvernements contractants à la Convention et par les installations portuaires; et d'un ensemble de directives publiées en 2012, constituées du Guide de la sécurité maritime et du Code. L'OMI a également élaboré un certain nombre de modules de formation sur la sécurité des navires et des ports, notamment la conduite de simulations et d'exercices, qui sont mis à la disposition des gouvernements membres sur demande. Nous nous sommes également dotés d'un programme dynamique d'activités de coopération technique qui vise à aider les États Membres à renforcer leurs capacités s'agissant de décourager, prévenir et détecter les menaces à la sécurité et d'y faire face, qui s'inscrit dans le prolongement du thème retenu pour la Journée mondiale de la mer en 2007 : « OMI : Connecter navires, ports et personnes ».

Le monde a beaucoup changé depuis que les mesures spéciales pour renforcer la sécurité maritime ont été introduites. Les menaces persistantes qui pèsent sur les secteurs portuaire, maritime et offshore et les infrastructures connexes continuent d'évoluer. Les ripostes à ces défis ont aussi évolué. Les objectifs du Millénaire pour le développement pour les pays en développement ont été remplacés par les objectifs de développement durable qui s'appliquent à l'échelle mondiale. Dans ce contexte, l'OMI aide activement les États dans le cadre de l'objectif de développement durable 9 pour bâtir une infrastructure résiliente et en ce qui concerne d'autres objectifs de développement durable importants. Les efforts ne se concentrent plus sur la lutte contre le terrorisme, mais l'accent est désormais mis sur des mesures à caractère anticipatif visant à prévenir le terrorisme.

Il convient de porter l'attention voulue aux possibilités offertes par le secteur maritime. Il faut considérer les ports et les navires comme une source de richesses dans le contexte du développement économique. À cet égard, une sûreté et une sécurité portuaires efficaces et efficientes sont désormais des éléments de plus en plus importants et pour lesquels on peut trouver des débouchés.

L'un des principaux défis à la mise en œuvre efficace des mesures de sécurité maritime et d'application de la loi dans le secteur maritime est que celles-ci sont considérées comme des questions relevant de différentes entités – des questions qui concernent la marine, la garde côtière, la police, les autorités portuaires, les autorités maritimes ou les douanes et les services chargés du contrôle aux frontières – qui se font concurrence pour des ressources limitées, et non de questions qui s'inscrivent dans une stratégie nationale multi-institutions face à un secteur portuaire et maritime en plein essor.

Par l'entremise de notre programme d'initiatives de renforcement des capacités visant à renforcer la sécurité maritime, l'OMI entend coopérer avec les pays développés et en développement, l'industrie maritime et les ports publics et privés pour promouvoir les pratiques exemplaires et jeter des ponts entre les divers acteurs. Au niveau national, il s'agit notamment d'améliorer l'efficacité du secteur maritime dans son ensemble en renforçant la coopération entre les ports et les navires et en resserrant les partenariats entre ces deux secteurs; d'améliorer les normes mondiales et d'établir des normes pour la sécurité, la sûreté et l'efficacité des ports et des services nationaux chargés des ports et des côtes; et d'améliorer la normalisation des procédures portuaires

en concevant et en élaborant des guides de pratiques exemplaires et du matériel didactique.

S’agissant du développement à long terme du secteur maritime dans son ensemble, les programmes de l’OMI – notamment notre appui au processus de Yaoundé en Afrique de l’Ouest et en Afrique centrale, conformément aux résolutions 2018 (2011) et 2039 (2012), et à l’Amendement de Djeddah au Code de conduite de Djibouti, adopté en janvier 2017 – s’emploient à remédier à l’absence de vision pour ce qui est des possibilités offertes par les océans et à encourager les investissements dans l’ensemble du secteur maritime. Nous encourageons notamment les autorités nationales à briser les cloisonnements pour passer d’une approche départementale à une approche nationale et à coopérer avec le secteur privé. Nous devons non seulement encourager la prise en compte des contributions du secteur portuaire aux plans d’action nationaux dans le secteur maritime et aux stratégies nationales et régionales maritimes et de sécurité maritime, mais également promouvoir le concept de port en tant que prestataire de services aux navires, pour mettre fin à cette attitude fondée sur la distinction entre « nous » et « eux ».

Pour ce faire, il est essentiel que les gouvernements nationaux renforcent leurs capacités de contrôle, de sûreté et de sécurité et promeuvent l’application du Code et du Code de pratique OIT/OMI pour les ports et les installations offshore. Cela inclut d’encourager la mise en place de comités consultatifs de facilitation et de sûreté des ports comme moyen de coopération interinstitutions aux fins d’une sécurité plus large – lutte contre toutes les menaces liées à la sécurité, notamment le vol, le trafic de drogues et d’espèces végétales et animales protégées, l’embarquement clandestin, la traite des migrants, le terrorisme – le tout sous contrôle gouvernemental afin d’en assurer l’efficacité, approche qui vaut aussi pour la protection des infrastructures essentielles d’autres secteurs.

Des systèmes de sécurité efficaces requièrent des procédures efficaces, un équipement approprié et, surtout, un personnel bien formé et motivé. Au niveau le plus bas, cela inclut la nécessité de mettre en œuvre des cadres et de mettre au point des outils pour mieux sensibiliser tout le personnel à la question de la sécurité. Toutefois, pour garantir l’efficacité et la durabilité des systèmes de sécurité, les gouvernements et le secteur portuaire doivent faire de la sécurité portuaire une carrière, non de simples emplois, en plaçant l’accent sur l’élaboration de programmes et de cours de formation assortis de la remise de diplômes pour permettre au personnel de passer du rôle de patrouilleurs et de gardiens à celui de superviseurs et de gestionnaires. On gagnerait aussi énormément à développer des réseaux d’officiers chargés de la sécurité des installations portuaires pour les aider à échanger les pratiques optimales et apprendre les uns des autres.

Bien que les deux moyens de transport diffèrent, il existe de nombreuses similitudes entre la sécurité aérienne et la sécurité maritime, notamment l’importance que les États membres adoptent une approche multiorganisations et engageant toutes les branches du gouvernement s’agissant d’organiser la sécurité, y compris la protection de l’infrastructure essentielle; l’importance de prendre en considération le système de sécurité dans son ensemble, à savoir l’évaluation des menaces, des risques et des vulnérabilités; la sélection, la formation et la certification du personnel; et l’équipement, les procédures et une supervision globale. On peut y ajouter la nécessité de planifier les interventions d’urgence et de renforcer la résilience; et d’assurer la protection des systèmes et des infrastructures de transport, vus comme un habilitant du développement économique, contribuant ainsi à la réalisation des objectifs de développement durable et à la prévention de l’extrémisme violent.

Comme on l’a souligné, les initiatives de sécurité maritime de l’OMI, menées en coopération avec l’Office des Nations Unies contre la drogue et le crime, INTERPOL et d’autres, promeuvent ces approches et, en particulier, encouragent la mise en place de comités nationaux pour la sécurité et la facilitation maritimes et l’élaboration de plans nationaux de sécurité et de plans d’intervention d’urgence approuvés au plus haut niveau, ainsi que la communication régionale entre les points de contact nationaux et la mise au point de programmes de formation et de certification plus détaillés pour le personnel travaillant au niveau des points clefs nationaux.

Le Président (*parle en anglais*) : Je remercie M. Trelawny de son exposé.

Je donne maintenant la parole à M. Heinonen.

M. Heinonen (*parle en anglais*) : Je me félicite de l’occasion qui m’est donnée aujourd’hui de partager certaines de mes réflexions personnelles sur le terrorisme nucléaire avec le Conseil de sécurité. Je voudrais plus précisément aborder cette question dans

la mesure où elle concerne l’Agence internationale de l’énergie atomique (AIEA) et le Conseil de sécurité. À cette fin, j’ai remis au Secrétariat une copie de la version intégrale de ma déclaration, qui contient des informations complémentaires appuyant certains points que je vais soulever aujourd’hui.

Nous savons tous qu’un accident nucléaire où qu’il survienne est un accident nucléaire qui nous affecte tous; il en est de même pour les répercussions du terrorisme nucléaire. Nous devons nous estimer heureux de n’avoir pas eu à souffrir jusqu’ici d’actes de terrorisme nucléaire, mais nous devons garder à l’esprit que les terroristes ont déjà publiquement fait part de leur volonté d’acquérir des armes nucléaires. Les vols et autres tentatives d’acquérir des matières nucléaires et radioactives montrent que cela pourrait se produire dans certaines conditions. La sécurité nucléaire peut être aussi compromise par d’autres moyens. Par exemple, le secteur de l’énergie a été victime de cyberattaques, notamment d’actes de sabotage d’installations nucléaires, au sujet desquels ma déclaration écrite comporte des preuves littérales.

Il y existe deux raisons qui font que la risque de terrorisme nucléaire est plus élevé aujourd’hui. La première est l’utilisation accrue et généralisée de la technologie nucléaire aux fins de la production d’électricité, de la technologie des rayonnements dans les secteurs médical et industriel, et l’expédition par bateau de matières radioactives et nucléaires à travers les frontières et les mers. Tout cela accroît le nombre d’installations physiques et de cargaisons maritimes, qui pourraient être des cibles potentielles d’attaques terroristes ou de vol. La deuxième raison a trait à un phénomène nouveau. Les organisations terroristes deviennent de plus en plus sophistiquées. Un récent rapport du Conflict Armament Research décrivant la production de munitions par l’État islamique d’Iraq et du Levant (EIIL) reflète une approche professionnelle incluant des contrôles de qualité de la production de ses engins. En d’autres termes, l’EIIL est capable d’attirer des ingénieurs compétents et autres spécialistes pour mener ses activités de production et pour s’approprier des modes perfectionnés de fonctionnement et de production. Voilà pourquoi nous ne devons pas ignorer la possibilité que ces organisations soient capables de recruter, ou du moins de chercher à coopter, des individus compétents en matière nucléaire, qui pourraient menacer les installations nucléaires du fait de leurs qualifications ou accroître la possibilité de faire exploser des bombes sales, par exemple.

Dans le même temps, quand nous considérons la possibilité que des actes de terrorisme nucléaire soient commis, nous ne devons pas nous limiter à des modes de pensée traditionnels s’agissant de la façon dont de tels actes peuvent survenir ou être menés. Par exemple, tout comme des matériaux nucléaires peuvent être utilisés pour fabriquer des bombes sales, la possession de ces matériaux toxiques peut tout aussi bien être utilisée à des fins de chantage ou impliquer leur dissémination dans des environnements urbains. À cet égard, nous ne pouvons que nous rappeler la tentative de contamination des réserves en eau de Damas ces dernières semaines. Des matériaux radioactifs pourraient être utilisés à des fins similaires.

Les menaces de terrorisme nucléaire peuvent émaner de diverses sources : organisations terroristes sophistiquées et bien financées, trafiquants de matières nucléaires, hackers capables de lancer des cyberattaques dévastatrices, et individus malintentionnés ayant accès à des informations d’initiés sur les installations nucléaires. Nous devons être prêts à contrer cet éventail de menaces, sous divers angles et scénarios. S’agissant du fonctionnement des installations nucléaires, tous ces défis ont une incidence sur leur gestion par les responsables d’une installation et par les personnes chargées de la règlementation et de la planification des interventions d’urgence. Certes, chaque État est responsable de la sûreté et de la sécurité nucléaires sur son propre territoire, mais nous devons êtres préparés en cas d’accidents, de situations d’urgence et d’incidents dont les effets sont ressentis au-delà des frontières, et notamment à gérer des situations d’urgence découlant du transport de matières nucléaires et radioactives à travers le territoire d’un État ou à proximité. Les capacités de préparation et d’intervention doivent aussi couvrir les incidents et les situations d’urgence découlant d’éventuels actes terroristes menés à l’aide de matériaux ne provenant pas de l’État visé.

Je voudrais appeler l’attention du Conseil sur un autre aspect sensible. Nous devons savoir que toute évaluation de la sécurité nucléaire en rapport avec l’utilisation de matières nucléaires ou radioactives dans le cadre d’applications militaires dans les États dotés d’armes nucléaires reste hors du contrôle de la communauté internationale dans l’état actuel des choses.

Il existe de nombreuses façons dont les États peuvent aborder la question et savoir quels sont les meilleurs moyens de lutter contre le terrorisme nucléaire. Il y a notamment la coopération étroite

entre les régimes de sécurité et de sûreté nucléaires et l'évolution des rôles joués par l'AIEA et l'ONU. Si la liste suivante n'est nullement exhaustive, elle donne de bonnes indications sur la voie à suivre. Les garanties, la sécurité et la sûreté sont généralement perçues comme des domaines distincts de la gouvernance nucléaire. S'il existe des raisons techniques et juridiques pour justifier cela, les trois perspectives peuvent aussi à bien des égards coexister et se renforcer mutuellement. Elles ont des effets synergétiques l'une sur l'autre, et les possibilités de collaboration doivent être identifiées afin de contribuer à l'efficience et à l'efficacité de l'ordre nucléaire global.

Les traités, les conventions et les codes de conduite non juridiquement contraignants de l'AIEA et les résolutions pertinentes du Conseil de sécurité, ainsi que la mise en commun des pratiques optimales et des ressources, sont tous considérés aujourd'hui comme partie intégrante des normes nucléaires mondiales. Toutefois, ce qui est adopté sur papier diffère de ce qui est fait dans la pratique. On pourrait envisager la possibilité d'établir un processus d'examen de ces instruments juridiques ou mécanismes afin de réaliser une évaluation plus transparente de la mise en œuvre par les États de leurs obligations. Cependant, avant de pouvoir le faire, d'autres mesures sont nécessaires, à commencer par un engagement plus actif de l'AIEA. Par exemple, le Directeur général de l'AIEA pourrait informer par écrit l'État concerné des risques pouvant découler d'une mise en œuvre inadéquate de ses engagements juridiques en vertu des instruments adoptés, ce qui permettrait d'ouvrir la voie à des mesures correctives.

Les modifications proposées pourraient être engagées de diverses façons. Le Conseil des gouverneurs de l'AIEA pourrait demander au secrétariat d'intervenir. Les États parties aux conventions sur la sûreté et la sécurité nucléaires pourraient également en prendre l'initiative lors des réunions d'examen de ces instruments. La prochaine Conférence internationale sur la protection physique des matières et installations nucléaires, qui doit se tenir en novembre, constitue une autre occasion de se pencher sur la façon de renforcer les infrastructures nucléaires contre les actes de terrorisme.

Les Sommets sur la sécurité nucléaire ont apporté des contributions importantes pour faire face aux menaces pesant sur la sécurité nucléaire, y compris les actes de terrorisme. Ces travaux se poursuivent dans une large mesure au sein de l'AIEA, en coopération avec d'autres organisations internationales et le secteur industriel, conformément aux résultats de la Conférence ministérielle de l'AIEA, tenue à Vienne en décembre 2016, qui a réaffirmé l'importance de la protection des matières nucléaires et radioactives. La Conférence a adopté une déclaration qui confère cette responsabilité à la communauté internationale, aux organisations internationales et aux États Membres. Afin de s'acquitter de cette obligation, l'AIEA et les autres organisations internationales ont besoin d'un financement adéquat. À cet effet, l'appui du Conseil de sécurité est indispensable. Les efforts déployés par celui-ci pour analyser et évaluer les menaces terroristes, mettre en lumière les vulnérabilités existantes, recenser les lacunes en matière de capacités afin de mieux cerner les défis que représente le terrorisme pour les infrastructures essentielles, et formuler des recommandations sur la façon d'appuyer au mieux les États Membres de l'ONU dans ce domaine, sont indispensables à la lutte contre le terrorisme.

Le Président (*parle en anglais*) : Je remercie M. Heinonen de son exposé.

Je vais maintenant faire une déclaration en ma qualité de Ministre des affaires étrangères de l'Ukraine.

Je tiens à remercier les personnes qui ont fait des exposés aujourd'hui de leur contribution à notre débat. Elles ont reconfirmé une fois de plus la complexité et l'importance de la problématique dont nous sommes saisis.

La protection des infrastructures essentielles est vitale pour la sécurité nationale, la sûreté publique et le développement économique de tous les États. Les attentats terroristes contre ces installations et services peuvent perturber gravement le fonctionnement des sociétés et provoquer d'immenses souffrances humaines.

Je voudrais également remercier tous les membres du Conseil de sécurité de leur appui lors de l'élaboration du texte de la résolution 2341 (2017) qui a été adoptée aujourd'hui. La résolution envoie un message fort de la part du Conseil de sécurité à la communauté internationale en lui demandant d'examiner sérieusement cette question. Elle établit également un cadre spécifique d'objectifs et de mesures afin de sensibiliser aux menaces terroristes qui peuvent viser les infrastructures essentielles en identifiant ces menaces, en s'attachant à les prévenir et en cherchant à atténuer leurs conséquences éventuelles.

Dans le cadre de leurs efforts indispensables en matière de lutte contre le terrorisme, les États

doivent impérativement élaborer et mettre en place une stratégie qui définit les tâches et les responsabilités correspondantes afin de protéger les infrastructures essentielles contre les attaques terroristes. Ses objectifs principaux doivent être de lutter contre ces attaques, d’empêcher qu’elles ne se reproduisent en identifiant les auteurs ainsi que leurs partisans et d’apporter une aide aux victimes du terrorisme.

Compte tenu des défis qui se posent actuellement à la paix et à la sécurité internationales, en particulier l’évolution des menaces terroristes, l’Ukraine œuvre à l’élaboration d’un cadre juridique national qui vise à protéger les infrastructures essentielles contre ces menaces. Ce travail est devenu particulièrement important étant donné la série d’attentats terroristes qui ont été commis contre des installations en Ukraine ces dernières années.

Depuis 2015, plusieurs organismes gouvernementaux ukrainiens ainsi que des infrastructures nationales essentielles, telles que des réseaux électriques régionaux et des institutions financières, ont été la cible d’attaques par des logiciels malveillants. Des groupes de hackers ont également attaqué l’aéroport de Kiev et les ressources électroniques du Ministère de la défense. Le 6 décembre 2016, à la veille de la fin de l’exercice, les sites Web du Trésor public, du Ministère des finances et de la Caisse des pensions de l’État ont été temporairement paralysés. Bien sûr, nous savons que ces attaques visent à perturber le système financier de l’Ukraine, à affaiblir nos capacités de défense et, à terme, à déstabiliser la société ukrainienne. Il est tout à fait évident que l’Ukraine a été délibérément choisie comme cible par des cyber-terroristes extérieurs organisés, dont les attaques peuvent être tout aussi dévastatrices qu’une guerre plus conventionnelle. Nous avons été touchés mais, du fait de ces attaques, nous sommes devenus plus résilients.

À l’heure d’une mondialisation en évolution rapide, nous pensons que les éléments ci-après doivent être incorporés dans les politiques nationales afin d’assurer un niveau suffisant de sécurité et de résilience des infrastructures essentielles. Le premier élément est la coopération entre toutes les parties prenantes, tant publiques que privées, qui interviennent dans l’exploitation et la protection des infrastructures essentielles. Le deuxième élément est un échange libre d’informations entre les autorités publiques, le secteur privé, les communautés et les citoyens sur les menaces et les risques visant les infrastructures essentielles. Le troisième élément est le renforcement du niveau d’autoprotection, d’assistance mutuelle et d’autonomisation des personnes et des organisations qui peuvent être touchées par l’élimination ou la perturbation d’infrastructures essentielles.

Outre les facteurs que je viens d’énumérer, un système qui veut s’attaquer de manière cohérente aux menaces terroristes visant les infrastructures essentielles doit accorder la priorité à une coopération internationale active, qui comprendrait, entre autres, la mise en commun des meilleures pratiques et la réalisation de formations et d’enquêtes conjointes. Cette coopération internationale est de plus en plus incontournable étant donné la réalisation de projets d’infrastructures transfrontières à l’échelle mondiale. Les attentats terroristes contre ces cibles peuvent avoir une incidence sur les intérêts de plusieurs États et causer des dommages importants à la fois à l’économie et à l’environnement. Dans ce contexte, notre objectif doit être d’intensifier la coopération aux niveaux national, régional et international et de mettre en place des mécanismes d’alerte et de réaction rapides afin de mieux faire face à d’éventuelles attaques terroristes.

Cela étant, tout en cherchant à protéger les parties les plus vulnérables de nos infrastructures essentielles contre les attaques terroristes, nous ne devons jamais oublier que c’est la vie de nos citoyens qui est en jeu et que nous, en tant qu’États, sommes tenus de les protéger. Par conséquent, il est de notre devoir de faire tout ce qui est en notre pouvoir pour prévenir les attaques terroristes contre les infrastructures essentielles. Le bien-être de nos peuples en dépend. C’est l’objectif principal de la résolution que nous avons adoptée aujourd’hui. Comme le dit le proverbe latin, *praemonitus praemunitus* : un homme averti en vaut deux. Je compte sur la poursuite de la coopération du Conseil en la matière.

Je reprends à présent mes fonctions de Président du Conseil.

Je donne maintenant la parole aux autres membres du Conseil de sécurité.

M. Amendola (Italie) (*parle en anglais*) : C’est un grand plaisir pour moi que d’être ici aujourd’hui pour prendre part à ce débat sur une question aussi cruciale. Je tiens à remercier le Ministre Klimkin d’avoir convoqué le débat public d’aujourd’hui et présenté la résolution 2341 (2017) au Conseil de sécurité pour adoption.

La menace posée par le terrorisme et la nécessité de protéger les infrastructures essentielles illustrent

à la perfection la complexité des défis auxquels nous sommes tous confrontés de nos jours en matière de sécurité. Le Conseil de sécurité a appelé à la mise en place d’une approche globale et préventive pour faire face aux effets potentiels sur la sécurité mondiale. La sécurité suppose la résilience des États et la cohésion de l’opinion publique. De fait, la résolution 2341 (2017) va permettre à la communauté internationale de combler un grand vide à cet égard. L’Italie se félicite donc de cette initiative et l’appuie.

Comme d’autres orateurs qui en ont fait l’expérience l’ont souligné, les terroristes s’en prennent aux infrastructures essentielles de très nombreuses façons et parfois, ils réussissent à perturber notre mode de vie. Le problème qui se pose est celui de la résilience de l’État, de la mobilisation de la population et de la peur que les terroristes diffusent dans nos sociétés. L’an dernier, par exemple, les attaques terroristes contre les aéroports de Bruxelles et d’Istanbul ont montré à quel point les groupes terroristes peuvent être efficaces et sans pitié. Les installations ciblées par Daech en Iraq dans le but de les exploiter sont un autre exemple manifeste, bien que d’un ordre différent, des dommages que les attaques peuvent causer aux infrastructures essentielles. Pour ce qui est de l’Iraq, l’Italie reste déterminée à protéger – comme elle le fait déjà avec fierté – le barrage de Mossoul, dont Daech cherche à s’emparer depuis 2014, mettant ainsi en péril la vie de centaines de milliers de personnes vivant dans les alentours.

Ce ne sont là que quelques exemples, mais leur impact montre à quel point il est vital que la communauté internationale agisse rapidement face à cette menace. Nous sommes en présence d’une menace transnationale qui appelle une riposte transnationale. De toute évidence, l’ONU a un rôle de premier plan à jouer – ce qu’elle fait d’ailleurs aujourd’hui – s’agissant de faire prendre conscience de la nécessité de coopérer au niveau international et de coordonner une action cohérente, y compris en s’appuyant sur les organisations régionales. Avant toute chose, nous devons déterminer quelles sont les cibles critiques. Deuxièmement, nous devons créer des synergies transfrontières afin de prévenir les attaques terroristes et d’en atténuer les effets. Troisièmement, nous devons repousser les menaces en coopérant entre États et le long de nos frontières. Dans la mesure où la force d’une chaîne dépend de son maillon le plus faible, le dialogue international, le partenariat, la mobilisation de l’opinion publique et le renforcement des capacités sont des éléments déterminants pour la protection des infrastructures essentielles.

Comme de nombreux orateurs l’ont déjà mentionné, au stade actuel des relations internationales, l’importance des connexions signifie que les infrastructures qui relient les gens entre eux ont, bien souvent, des incidences sur la société par-delà les frontières. Parfois ces liens sont plus forts que les frontières, et lorsqu’il s’agit de respecter ou de défendre les frontières, nous devons tenir compte de la nécessité que les nations coopèrent à la défense de ces liens. C’est pourquoi nous sommes prêts à appuyer le rôle de l’ONU, comme le suggère la résolution, pour recenser et diffuser les bonnes pratiques en matière de protection de ces infrastructures.

Un élément clef de partenariat est le partage de l’information. Nous le savons bien en Europe – c’est d’ailleurs ce que nous faisons dans le cadre de l’Union européenne –, mais tous les États Membres devraient être tenus au courant de la nature des menaces qui visent un pays donné lorsque celles-ci portent atteinte à notre sécurité collective.

Qu’il me soit permis de dire quelques mots sur le rôle et l’importance du cyberespace, et plus généralement des technologies de l’information et des communications. Nous savons que, de nos jours, elles revêtent une importance décisive pour nos infrastructures et qu’elles sont à la fois un outil et une cible des terroristes. Nous pensons que nous devons mieux comprendre ce qui constitue une attaque contre les technologies de l’information et des communications. Le fait de ne pas être capable de détecter ou de stopper la planification en ligne d’attentats ou la propagande des groupes terroristes sur Internet est déjà une attaque en soi. Les détournements d’avion ou de camion sont considérés comme des attaques, et de la même manière nous devons reconnaître que lorsque les réseaux informatiques sont détournés par des organisations terroristes il s’agit aussi d’une attaque, même si elle est d’un autre genre. Nous devons trouver un équilibre entre liberté d’accès pour l’opinion publique et la société civile, car c’est un extraordinaire outil de communication et de participation démocratique, et sécurité collective. Ce n’est pas facile, mais la résolution d’aujourd’hui va permettre d’améliorer les efforts en faveur de notre liberté et de notre sécurité.

Cela m’amène à la nouvelle alliance que nous devons encourager et forger. À cet égard, défendre les infrastructures essentielles passe aussi par une alliance

entre le secteur public et le secteur privé, parce que les connexions qui stimulent le commerce, les affaires et les communications sont aussi celles qui permettent le dialogue au sein de la société civile ainsi que la défense et la protection de notre sécurité. C’est pourquoi le débat et la résolution d’aujourd’hui sont importants. Ils proposent en effet un cadre juridique international indispensable pour la mise en place et le développement d’un tel partenariat au sein d’une société libre, ouverte et inventive.

M. Abdymomunov (Kazakhstan) (*parle en anglais*) : Je tiens à vous remercier, Monsieur le Président, de mettre ainsi un coup de projecteur sur la nécessité de protéger les infrastructures essentielles face aux récents changements dans les tactiques et stratégies employées et les formes prises par les organisations terroristes de nos jours. Le défi se pose avec d’autant plus d’acuité que les infrastructures essentielles qui sont vulnérables couvrent des champs d’activités et des catégories extrêmement vastes, puisqu’elles vont des installations nucléaires et énergiques, au commerce, à la finance et au secteur bancaire en passant par toutes les formes de transport, pour n’en citer que quelques-uns. Le problème est de surcroît exacerbé par le fait que l’informatique et les technologies de l’information et des communications modernes sont au cœur même du fonctionnement de plus d’une vingtaine de grands systèmes d’infrastructures essentielles ayant des ramifications nationales, régionales et mondiales.

Ma délégation voudrait présenter ici les précautions que prend le Kazakhstan sur deux fronts très importants, le premier, les technologies de l’information et des communications appliquées aux ressources publiques, et le deuxième, les installations nucléaires.

Le Kazakhstan est conscient que les infrastructures essentielles modernes suscitent la convoitise des organisations terroristes internationales et sont la cible de leurs attaques. Bien que la protection des infrastructure relève de la responsabilité directe des autorités publiques, nous estimons que des efforts conjoints entre le secteur public et le secteur privé s’imposent, parallèlement à une coopération étroite avec les organisations internationales et régionales, y compris l’Office des Nations Unies contre la drogue et le crime, l’Agence internationale de l’énergie atomique, INTERPOL, l’Organisation pour la sécurité et la coopération en Europe, l’OTAN ainsi que l’Organisation de Shanghai pour la coopération et l’Organisation du Traité de sécurité collective.

Nous sommes également attentifs aux risques potentiels de catastrophe dans les domaines de l’énergie et des affaires ainsi qu’aux risques de catastrophes transfrontières et transnationales, en raison des liens qui unissent ces secteurs par technologies de l’information et des communications interposées. Face à ces circonstances, nous sommes en train de développer notre système national de lutte contre le terrorisme sur Internet, qui est baptisé « Bouclier cybernétique du Kazakhstan ».

À l’heure actuelle, les législations des États Membres n’incluent pas une définition harmonisée de ce qu’est une infrastructure essentielle, et il est donc indispensable d’uniformiser les législations nationales pour qu’elles répondent aux normes mondiales établies par les Nations Unies en matière de sécurité des infrastructures essentielles.

J’en viens maintenant à un autre aspect clef des infrastructures essentielles, les infrastructures nucléaires. La sûreté nucléaire est une responsabilité collective fondamentale de nos jours aux niveaux national, régional et mondial. Le Kazakhstan prend donc toutes les mesures qui s’imposent pour garantir la sécurité des installations nucléaires situées sur son sol et dans sa région. Nous sommes partie à presque toutes les conventions internationales dans ce domaine et appelons les autres États à respecter et appliquer ces instruments en toute bonne foi.

Nous nous employons aussi activement à promouvoir un cadre juridique international garantissant le traitement sûr des matières nucléaires. Nous avons à cœur de protéger les infrastructures essentielles, notamment celles situées sur l’ancien site d’essais nucléaires de Semipalatinsk, aujourd’hui Centre nucléaire national de la République du Kazakhstan, ainsi que le réacteur nucléaire BN-350, avec le soutien actif de nos partenaires. Nous sommes prêts à former des spécialistes hautement qualifiés et, dans cette optique, nous mettons en place à Almaty, avec l’appui de l’Agence internationale de l’énergie atomique (AIEA) et du Gouvernement des États-Unis, des centres de formation à la sûreté nucléaire.

Nous prenons des mesures strictes en vue d’assurer que l’établissement d’une banque d’uranium faiblement enrichi et le transport de matières nucléaires sur notre territoire se fassent dans des conditions de sécurité. À cet égard, je rappelle que le Kazakhstan a satisfait aux prescriptions des quatre Sommets sur la sécurité nucléaire, notamment pour ce qui est d’une

utilisation sûre de l'énergie nucléaire. Nous nous attelons également à sécuriser les sources radioactives que des terroristes pourraient utiliser pour fabriquer des armes à matière radioactive ou bombes sales.

Tous les efforts ont été déployés pour assurer la sécurité des 28e Universiades d'hiver, organisées récemment à Almaty, l'accent ayant été mis sur l'identification et l'élimination précoces des menaces. Il en va de même pour la prochaine EXPO 2017 d'Astana.

Je suis heureux d'annoncer que nous établissons une coopération étroite avec le Programme européen pour la protection des infrastructures critiques, en même temps que nous luttons contre les crimes transnationaux. Le pays est également actif au sein du Réseau d'alerte concernant les infrastructures critiques de la Commission européenne, partageant des informations sur la recherche en matière de protection des infrastructures.

Le Kazakhstan est prêt à mettre au point des systèmes de sécurité communs, acceptables pour tous les États, quelles que soient leurs caractéristiques et leurs traditions nationales, afin de préserver notre monde et notre planète des menaces toujours croissantes auxquelles nous sommes confrontés.

M. Skoog (Suède) (*parle en anglais*) : Je voudrais tout d'abord remercier la présidence ukrainienne du Conseil de sécurité d'avoir convoqué le présent débat public et d'avoir tenu des consultations sur la résolution 2341 (2017) que nous venons d'adopter. Le consensus dont elle fait l'objet met en relief le processus transparent et inclusif qui a abouti à ce résultat, ainsi que l'importance que nous attachons tous à cette question vitale. Par respect pour tous les États Membres qui veulent participer à ce débat, je vais faire maintenant une déclaration abrégée et rendre la version complète disponible par d'autres moyens.

Les infrastructures essentielles sont depuis longtemps des cibles de choix pour les attaques terroristes. En coupant l'électricité, en contaminant ou en fermant l'approvisionnement en eau, ou en sapant la volonté des individus de voyager, de telles attaques atteignent l'objectif principal du terrorisme qui est de susciter autant de peurs et de perturbations que possible. Il est difficile d'imaginer les conséquences dévastatrices qu'une attaque terroriste sur une centrale nucléaire pourrait avoir sur les vies humaines et sur l'environnement, tant en termes d'impact immédiat que d'effets à long terme. M. Heinonen nous a rappelé que ce n'est pas un scénario totalement irréaliste.

Nous vivons dans un monde de plus en plus interconnecté. Cela est particulièrement vrai quand il s'agit de notre infrastructure critique. L'interconnexion – qu'elle soit physique ou en termes de technologie des communications – signifie que les répercussions d'une attaque massive dans un pays peuvent être ressenties non seulement dans les pays voisins, mais mondialement. C'est pourquoi ce débat est d'autant plus opportun et pertinent. Les efforts visant à protéger les infrastructures essentielles des attaques terroristes nécessitent une coopération – à travers les frontières, entre les secteurs et entre les parties prenantes publiques et privées. Les approches régionales et mondiales contribuent à renforcer la résilience et le niveau de préparation. Tous les organismes publics suédois sont tenus d'entreprendre une analyse de la sécurité en vue d'identifier les infrastructures essentielles vitales relevant de leur compétence et de recenser et d'évaluer les risques potentiels.

Le but de notre politique est double. Le premier objectif est d'améliorer la sensibilisation, de renforcer la résilience et de prévenir les attaques, de réagir et de se relever des incidents et des crises où qu'ils se produisent. Le deuxième objectif est d'accroître la coopération en matière de prévention entre toutes les parties prenantes concernées, y compris les acteurs publics et privés, aux niveaux régional et international.

Le Conseil suédois de coopération antiterroriste rassemble les acteurs concernés afin d'accroître conjointement les capacités nationales. Notre approche implique les autorités chargées de l'application de la loi, du renseignement et de la sécurité, l'Agence pour la protection civile, les agences sectorielles, les autorités régionales et locales et les acteurs du secteur privé qui possèdent et exploitent des infrastructures essentielles. En 2016, nous avons lancé un système national de déclaration obligatoire des incidents dans le domaine de la technologie de l'information à l'intention de tous les organismes gouvernementaux. L'année prochaine, dans le cadre de la directive de l'Union européenne (UE) sur la sécurité des systèmes d'information sur réseaux, ces rapports deviendront obligatoires pour les acteurs publics et privés.

En outre, au niveau de l'Union européenne, l'UE et ses États membres s'engagent à être solidaires de tout État membre faisant l'objet d'une attaque terroriste, au titre de la « clause de solidarité ». L'UE

a mis en place une série d'initiatives visant à protéger les infrastructures critiques. Cette approche est non seulement axée sur les menaces d'attaques terroristes, mais aussi sur celles résultant d'activités criminelles, de catastrophes naturelles et d'accidents. Nous soutenons plusieurs programmes de l'UE visant à protéger les infrastructures essentielles au sein de la région élargie, qui comprend les Balkans et la Turquie.

Il existe un certain nombre d'organisations régionales créées pour améliorer les capacités des États membres en matière de protection civile et de préparation, comme le Conseil des États de la mer Baltique, le Conseil de l'Arctique et le Conseil euroarctique de la mer de Barents, un forum dont l'objectif est de soutenir et de promouvoir la coopération régionale dans les régions les plus septentrionales de la Suède, de la Norvège, de la Finlande et du nord-ouest de la Russie. L'Islande et le Danemark en sont également membres.

Les auteurs d'actes de terrorisme doivent être traduits en justice, de même que les organisateurs et les commanditaires d'attentats terroristes doivent être tenus pour responsables. Comme le prévoit la résolution 2341 (2017) adoptée aujourd'hui, les mesures de lutte contre le terrorisme doivent être prises conformément au droit international, y compris le droit des droits de l'homme et le droit international humanitaire.

Nous nous félicitons du fait que la résolution encourage le Comité du Conseil de sécurité créé par la résolution 1373 (2001) concernant la lutte antiterroriste à continuer d'examiner ces questions importantes. Les visites de pays effectuées par la Direction exécutive du Comité contre le terrorisme ont produit des connaissances et une expertise précieuses qui donnent aux États la possibilité de tirer parti des meilleures pratiques. Une coopération internationale accrue – et non pas réduite – est essentielle pour contrer ces menaces. Nous apprécions le leadership de l'Ukraine sur ces questions au Conseil de sécurité.

M. Lamek (France) : Qu'il me soit permis en premier lieu de remercier l'Ukraine d'avoir pris l'initiative de ce débat important. Je voudrais également remercier les différents intervenants pour leurs présentations très éclairantes. La France s'associe au discours qui sera prononcé au nom de l'Union européenne.

Les exemples d'attaques terroristes ayant visé des infrastructures critiques, en particulier de transport, sont malheureusement nombreux, comme l'ont tragiquement rappelé les attentats perpétrés dans le métro et à l'aéroport de Bruxelles en mars 2016 et dans les aéroports d'Istanbul en décembre 2015 et juin 2016. Ce débat nous offre l'occasion de passer à nouveau un message fort, un message uni du Conseil de sécurité sur l'importance de la coopération internationale dans la lutte contre le terrorisme, comme nous l'avons déjà fait par le passé à l'occasion d'autres séances sur le financement du terrorisme, sur la lutte contre la propagande ou pour la coopération judiciaire internationale.

Cette lutte contre la menace terroriste doit porter sur tous les fronts, dans le respect du droit international et des compétences nationales des États. Il est en particulier nécessaire, au niveau de chaque pays, de se doter de moyens de prévention et de protection robustes, afin de dissuader les terroristes de mener des attaques contre des cibles potentiellement vulnérables, ou le cas échéant, afin de se trouver en mesure de réagir rapidement et efficacement.

La France fait de la protection de la population, ainsi que de la garantie de la continuité des fonctions essentielles de la nation une priorité stratégique. Elle a mis en place, dès 2006, un dispositif de sécurité des « activités d'importance vitale » afin de les protéger contre les actes de malveillance tels que le terrorisme. Aujourd'hui, ce sont plus de 200 opérateurs, publics et privés, qui ont été catégorisés « organisme d'importance vitale », qui font l'objet de règles et d'une vigilance particulières. La liste de ces infrastructures, gardée confidentielle, inclut des administrations, des médias, des entreprises de transports ou encore des industriels opérants dans différents secteurs. Tous assurent des activités indispensables au bon fonctionnement et à la survie de la nation.

Dans ce contexte, la France se réjouit de l'adoption à l'unanimité de la résolution 2341 (2017), la première qui s'intéresse de si près à cette thématique essentielle. Je tiens plus particulièrement à insister sur deux messages, particulièrement importants, que ce texte envoie.

Le premier concerne la prévention et la préparation aux éventuelles menaces. Il est indispensable d'identifier en amont les principaux défis et les vulnérabilités en matière de protection des infrastructures critiques, et d'élaborer une stratégie ciblée à mettre en place en cas d'attaque. Ces approches aident non seulement à réduire les risques, mais également à renforcer la réactivité.

Le second message porte sur le constat que le renforcement de la protection des infrastructures critiques ne peut se faire de manière isolée. La coopération,

qu'elle soit interagences ou interétatique, est essentielle afin de garantir un niveau de protection adapté. Cela passe notamment par l'échange d'informations, de connaissances et d'expériences. En raison de la nature même des activités assurées par ces infrastructures critiques, une coopération étroite entre le secteur public et le secteur privé est absolument indispensable.

Les défis sont nombreux. Mais l'ampleur et le niveau particulièrement élevé de la menace terroriste aujourd'hui doivent nous inciter à renforcer nos efforts de protection des populations et nos efforts de garantie de la continuité des services essentiels de l'État.

Permettez-moi, pour conclure, Monsieur le Président, de remercier à nouveau la présidence ukrainienne du Conseil de sécurité pour ce débat très utile sur une question à la fois spécialisée et technique, mais qui touche de près la vie quotidienne de nos concitoyens. Soyez assuré que la France continuera de prendre toute sa part à ces efforts.

M. Seck (Sénégal) : Vous me permettrez, à l'entame de mon propos, Monsieur le Président, de vous adresser les sincères remerciements de la délégation sénégalaise pour avoir pris l'initiative d'organiser ce débat combien important sur un thème dont l'importance et l'actualité sont avérées. De par leurs brillantes présentations, nos intervenants de ce matin, à savoir Mme Viotti, M. Stock, M. Rao et M. Trelawny, nous ont donné la pleine mesure de la problématique sous examen. Je voudrais, au nom de la délégation sénégalaise, les en remercier et les en féliciter chaleureusement.

Déjà, en septembre 2016, nous avions tenu ici-même un débat public relatif à la sécurité aérienne face aux attaques terroristes (voir S/PV.7775). Nous avions également tenu deux réunions en novembre, selon la formule Arria, organisées l'une par l'Ukraine, justement, sur le même sujet des infrastructures essentielles, et l'autre, coorganisée par le Sénégal et l'Espagne, sur la problématique de la cybersécurité. Aussi, nos échanges de ce matin nous offrent-ils l'opportunité de poursuivre la réflexion stratégique sur les voies et moyens de bien identifier, pour mieux les prévenir, les risques liés à ce type de menaces et de mesurer en même temps la fiabilité et la résistance, ou la vulnérabilité, des infrastructures essentielles face aux attaques terroristes pouvant engendrer des catastrophes incommensurables.

En effet, parce qu'elles deviennent de plus en plus la cible de groupes extrémistes, qui ont pour objectif de faire le plus grand nombre de victimes civiles possibles, les infrastructures essentielles doivent faire l'objet d'une surveillance et d'une protection prioritaires, afin de préserver le fonctionnement normal des communautés humaines et des entreprises, tout en garantissant la sécurité nationale et la sûreté publique dans les pays visés ou atteints. À cet égard, ma délégation se félicite de l'adoption à l'unanimité de la résolution 2341 (2017), qui constitue assurément un bon pas dans les efforts à fournir par la communauté internationale face à ces menaces émergentes à la paix et la sécurité internationales.

Compte tenu de l'interconnexion de ce type d'infrastructures, qui accentue leur vulnérabilité, la vigilance et la veille permanentes, fondées sur une prise en compte des spécificités propres au contexte et à l'environnement géopolitiques internes et externes de chaque pays et de chaque région, nous paraissent fondamentales. La délégation sénégalaise juge impératif d'établir et de renforcer des partenariats public-privé aux niveaux national, régional et international avec toutes les parties prenantes, aussi bien en matière de partage d'informations, d'expériences, de renseignements même, ainsi que de coordination opérationnelle, de sécurisation des chaînes d'approvisionnement et de contrôle des frontières. Il me plaît de rappeler que, pour sa part, le Sénégal a mis en place un cadre d'échange et de partage d'informations sensibles avec les autres États, dans le souci de faire face, de manière plus efficace, à la recrudescence des nouvelles menaces et tentatives d'actes d'intervention illicite utilisant des aéronefs ou visant des installations aéroportuaires ou portuaires.

Dans le domaine aéronautique, et en vertu des dispositions de l'Organisation de l'aviation civile internationale, qui stipulent que chaque État a la responsabilité de garantir une mise en œuvre efficace de toutes les mesures de sûreté visant à protéger l'aviation civile contre les actes d'intervention illicite, l'État du Sénégal a entrepris, depuis plusieurs années, un vaste programme de renforcement de la sécurité de l'aviation civile sur son territoire et dans son espace aérien. Cette politique a amené l'Assemblée nationale à adopter un nouveau code de l'aviation civile, par la loi n° 2015-10 du 4 mai 2015, et la mise en place de règlements aéronautiques pour encadrer la mise en œuvre opérationnelle des mesures et procédures de sûreté.

Dans le domaine maritime et portuaire, je voudrais indiquer que le Sénégal est partie prenante à la plupart des instruments internationaux évoqués par le Conseiller spécial du Secrétaire général de l'Organisation maritime

internationale, y compris le Processus de Yaoundé et le Code de conduite de Djibouti, sans oublier la Charte africaine sur la sûreté et la sécurité maritimes et le développement en Afrique, adoptée en octobre dernier à Lomé, en République togolaise.

Au plan sous-régional, un accord de coopération a été signé le 24 mars 2016 par les ministres compétents du Sénégal, du Mali, de la Côte d'Ivoire et du Burkina Faso à l'effet de mutualiser les efforts de leurs pays, de renforcer les relations de collaboration entre les services de sécurité et d'établir ainsi une unité d'action, en harmonisant les législations nationales en matière de lutte contre le terrorisme et les normes de surveillance des frontières, mais également pour assurer la fiabilité des documents de voyage, dans le respect des accords régionaux en matière de circulation des personnes.

L'Afrique de l'Ouest a connu, ces dernières années, une recrudescence d'attaques terroristes et des menaces d'attaque cybercriminelle. À ce sujet, les résultats de la mission onusienne d'évaluation des incidences de la crise libyenne sur la région du Sahel, conduite en décembre 2011 (voir S/2012/42), faisaient état de la circulation d'une grande quantité d'armes et de munitions, en particulier des lance-roquettes, dans la région. Passées en contrebande, ces armes représentent une réelle menace pour la sécurité et la stabilité dans la région sahélo-saharienne. Il est donc essentiel d'éviter que l'Afrique devienne le maillon faible de la prévention, de la protection et de la sécurisation des infrastructures essentielles. À ce sujet, la délégation sénégalaise se réjouit d'une mise en œuvre effective du paragraphe 9 de la résolution que nous venons d'adopter, et la soutient fortement.

De même, le Comité contre le terrorisme, qui effectue déjà un travail remarquable à travers sa Direction exécutive, en collaboration avec l'Équipe spéciale de lutte contre le terrorisme, devrait continuer à apporter son assistance technique aux États touchés, dans le renforcement de leurs capacités à protéger les infrastructures vitales, ainsi que les espaces publics vulnérables.

Pour conclure, ma délégation voudrait indiquer que, pour être efficace, la mise en œuvre de la résolution que nous venons d'adopter doit être en parfaite cohérence avec les résolutions précédemment adoptées par le Conseil dans le cadre de la lutte contre le terrorisme, notamment les résolutions 2178 (2014), 2253 (2015) et 2322 (2016), et s'inscrire ainsi dans le cadre plus global de la Stratégie antiterroriste mondiale des Nations Unies. Aussi, la délégation sénégalaise attend-elle avec beaucoup d'intérêt la présentation dans les 12 mois à venir, par le Comité contre le terrorisme, du niveau de mise en œuvre de l'importante résolution que nous avons adoptée.

M. Bessho (Japon) (*parle en anglais*) : Je tiens tout d'abord, Monsieur le Président, à vous adresser mes sincères remerciements pour avoir choisi d'aborder cette importante question d'actualité. Je remercie également Mme Viotti et tous les autres intervenants de leurs exposés instructifs.

Au cours des derniers mois, nous avons adopté deux résolutions du Conseil de sécurité sur la lutte contre le terrorisme : la résolution 2309 (2016), sur la sécurité de l'aviation, et la résolution 2322 (2016), sur la coopération internationale en matière judiciaire. Nous saluons l'adoption aujourd'hui de la résolution 2341 (2017), sur la protection des infrastructures essentielles. Nous remercions l'Ukraine d'avoir pris la tête de cette initiative. En adoptant ces résolutions, le Conseil de sécurité a su faire preuve d'unité pour s'attaquer au terrorisme au moyen d'une approche multiforme. Notre tâche consiste maintenant à appliquer concrètement ces résolutions.

Lorsque survient un acte de terrorisme, il est déjà trop tard, en particulier compte tenu des effets dévastateurs que la destruction d'infrastructures essentielles peut avoir sur les sociétés et les personnes. Nous devons renforcer collectivement notre sécurité en mettant l'accent sur la prévention. Le Japon accorde une priorité particulière à la protection des infrastructures essentielles. Nous le devons à la fois à nos citoyens et à nos visiteurs. Ceci est particulièrement pertinent pour le Japon, qui accueillera les Jeux olympiques et paralympiques à Tokyo en 2020 et la Coupe du monde de rugby en 2019.

En tirant parti des pratiques internationales optimales, le Japon a renforcé la sécurité de ses infrastructures, notamment les transports publics, les installations qui accueillent des manifestations de grande ampleur, les ports maritimes internationaux, les centrales nucléaires et les ambassades. La protection des centrales nucléaires contre les attaques terroristes revêt une importance particulière du fait des effets particulièrement dévastateurs que ce genre d'attaques pourrait avoir. En ce qui concerne les centrales nucléaires japonaises, des brigades anti-armes à feu sont déployées par la police 24 heures sur 24 et des groupes d'assaut spéciaux peuvent être mobilisés en cas d'urgence.

L'accès à l'information est essentiel. Le Japon échange des informations avec ses homologues étrangers, et les forces de police effectuent des exercices conjoints avec les forces d'autodéfense et collaborent étroitement avec les exploitants de centrales nucléaires, notamment par des visites sur le terrain et des conseils en matière de vigilance.

Il est crucial de s'adapter aux récentes avancées techniques. Compte tenu de l'augmentation du nombre d'incidents impliquant l'utilisation malveillante des technologies de l'information et des communications, le Japon est en train de renforcer sa cybersécurité en coopération avec le secteur privé et ses homologues étrangers. En avril dernier, nous avons promulgué une loi qui interdit aux engins sans pilote, ou drones, de survoler les installations essentielles, les ambassades et les centrales nucléaires afin de prévenir d'éventuelles attaques.

Nos expériences attestent de l'importance de la multiplication des efforts, notamment la coopération internationale et entre les secteurs public et privé, l'accélération de l'échange d'informations, le partage de bonnes pratiques, le développement de technologies de pointe et l'appui au renforcement des capacités pour ceux qui en ont besoin. Nous estimons que la résolution qui vient d'être adoptée constitue un cadre important pour permettre à tous les autres membres d'entreprendre des efforts dynamiques. Dans le cadre de ces efforts, il y a deux semaines, le Gouvernement japonais a adopté un nouveau programme d'aide pour la coopération internationale en matière de lutte contre le terrorisme et de prévention de l'extrémisme violent. Cela facilitera la mise en œuvre des résolutions pertinentes du Conseil de sécurité grâce à la mise en place de projets concrets, notamment un projet de lutte contre les cyberattaques visant les systèmes informatiques des infrastructures financières. Nous appuyons également l'initiative prise par le Secrétaire général Guterres de garantir la coordination et la cohérence de l'action antiterroriste menée par l'ONU, dans le cadre du processus d'examen de la Stratégie antiterroriste mondiale des Nations Unies.

Pour terminer, je tiens à souligner que le Japon est prêt à se mobiliser promptement et à tout moment contre le terrorisme sous tous ses aspects. Le Japon restera un partenaire actif de l'ensemble de la communauté internationale dans cette entreprise importante.

M. Alemu (Éthiopie) (*parle en anglais*) : Nous tenons à remercier la présidence ukrainienne d'avoir organisé cet important débat sur la protection des infrastructures essentielles contre les attaques terroristes et à vous remercier, Monsieur le Président, de le présider. Nous nous félicitons de l'adoption à l'unanimité de la résolution 2341 (2017) et remercions tous les intervenants de leurs présentations.

Compte tenu des menaces croissantes que posent le terrorisme et l'extrémisme violent, la vulnérabilité des infrastructures essentielles face à d'éventuelles attaques terroristes est une source de profonde préoccupation. Les effets dévastateurs dans les domaines économique et de la sécurité de telles attaques contre certaines infrastructures que nous considérons normalement comme acquises dans notre vie quotidienne, notamment l'eau, l'électricité, les télécommunications et Internet, les transports, les banques et les institutions financières, sont trop épouvantables pour être envisagés. Bien sûr, l'industrie aéronautique a souvent été la cible principale des terroristes, et de nombreuses mesures ont déjà été mises en place en vue d'améliorer la sécurité de l'aviation. Cependant, l'industrie aéronautique reste exposée aux attaques terroristes; d'où la nécessité de renforcer la coopération internationale pour combler toute faille que pourraient exploiter les terroristes.

Nous savons tous que les terroristes et autres criminels ont maintenant la capacité de lancer des attaques coordonnées et sophistiquées contre d'autres infrastructures essentielles. Les institutions publiques, les entreprises privées, les usines et les industries, les routes et les ponts, les centres commerciaux et les centres sportifs, entre autres, sont de plus en plus souvent des cibles d'attentats visant à perturber l'activité économique normale. Le cyberterrorisme, dont l'objectif est d'endommager les systèmes informatiques et les infrastructures de télécommunication, est également devenu un danger réel.

Tous les pays, petits et grands, sont exposés à ce type d'attaques. Étant donné que nous vivons dans une région instable, qui est confrontée aux menaces du terrorisme et de l'extrémisme violent, les attaques terroristes commises contre des infrastructures essentielles ne sont pas pour nous des possibilités théoriques. Elles constituent des menaces réelles et se sont déjà produites dans notre région. Nous estimons que c'est sur la base d'une coopération internationale efficace qu'il sera possible de renforcer la protection, la sécurité et la résilience des infrastructures essentielles.

On pourrait arguer que la question de la protection des infrastructures essentielles est en partie couverte par les conventions et traités internationaux

relatifs à l'aviation civile, à la sécurité maritime et aux armes nucléaires. Cependant, aucune résolution n'a été consacrée à cette question, et nous espérons que la résolution adoptée aujourd'hui contribuera pleinement à promouvoir le renforcement de la coopération internationale afin de lutter efficacement contre les attaques terroristes visant des infrastructures essentielles.

Comme le souligne à juste titre la note de cadrage (S/2017/104, annexe), il importe de renforcer les capacités nationales pour prévenir et endiguer les menaces et risques potentiels à cet égard. Le Comité contre le terrorisme, sa direction exécutive et l'Équipe spéciale de lutte contre le terrorisme vont jouer un rôle crucial dans le suivi de cette question et l'aide au renforcement des capacités des États Membres. L'élaboration par l'Équipe spéciale de programmes adaptés en matière de protection des infrastructures essentielles, en tenant compte des menaces potentielles et des risques auxquels sont exposés les pays, serait certainement très utile. La réactivation du Groupe de travail de l'Équipe spéciale sur la protection des infrastructures critiques, y compris Internet, les cibles vulnérables et la sécurité du tourisme sera indispensable pour atteindre cet objectif, comme le serait à n'en pas douter l'initiative bienvenue qu'envisage de mettre en place le Secrétaire général pour renforcer la capacité du Secrétariat à coordonner plus efficacement les efforts de lutte antiterroriste de l'ONU, qui manquent jusqu'à présent de cohérence.

Enfin, nous estimons que le partage d'expériences et de bonnes pratiques entre les pays et les régions pourrait aussi contribuer considérablement à renforcer les capacités et à favoriser la réactivité face à ces menaces. L'Organisation des Nations Unies, en coopération avec les organisations régionales et sous-régionales, pourrait faciliter la mise en place de ces mécanismes pour faire mieux connaître ces questions et favoriser le partage d'expériences utiles en matière de protection des infrastructures essentielles.

M. Bermúdez (Uruguay) (*parle en espagnol*) : Je vous remercie, Monsieur le Ministre, de présider nos travaux aujourd'hui. Je félicite votre pays d'avoir organisé ce débat public et d'avoir mené dans un esprit d'équilibre et en toute transparence les négociations sur l'importante résolution 2341 (2017) qui a été adoptée aujourd'hui, qui, avec la résolution 2309 (2016) relative aux menaces terroristes pesant sur l'aviation civile, atteste de l'importance que le Conseil attache à cette question. Je me félicite de la participation à la présente séance de la Directrice de cabinet du Secrétaire général, l'Ambassadrice Maria Luiza Ribeiro Viotti, ainsi que de tous les intervenants qui sont ici aujourd'hui. Je les remercie également de leurs exposés édifiants.

La communauté internationale est de plus en plus préoccupée par les menaces terroristes visant des infrastructures essentielles. Ces préoccupations sont tout à fait justifiées compte tenu des conséquences graves que de tels actes peuvent entraîner, en termes de pertes de vies humaines, de destruction ou de diminution de la capacité des États à fournir des services essentiels à la population et de pertes économiques. Les actes de groupes terroristes, qui utilisent les nouvelles technologies et qui disposent de capacités accrues, transcendent les frontières et les régions, ce qui nous oblige à prendre des mesures pour relever ces nouveaux défis. Il n'est donc pas étonnant qu'aux niveaux national, régional et international, les initiatives visant à protéger les infrastructures, qui tiennent compte aussi bien des aspects physiques que numériques, gagnent du terrain.

Il faut également sensibiliser le public sur les menaces cybernétiques et leurs conséquences éventuelles, en associant tous les acteurs publics et privés à ces efforts et en les encourageant à coopérer et à coordonner leurs activités. En outre, il ne fait aucun doute qu'il s'agit d'un domaine dans lequel il convient d'élaborer davantage de normes, tant au niveau national qu'international. Comme nous l'avons vu dans d'autres domaines en matière de lutte contre le terrorisme, la coopération entre les États et aux niveaux régional et international est d'une importance capitale pour l'efficacité des politiques visant à prévenir de telles attaques et à contenir leurs conséquences potentielles. Cela est de plus en plus nécessaire, car de nombreux États se heurtent à des difficultés et à des contraintes pour élaborer et mettre en œuvre des politiques efficaces, faute de ressources matérielles ainsi que de personnel qualifié et d'expérience en matière d'évaluation de menaces, de risques, de vulnérabilités et de conséquences. Par conséquent, il convient de renforcer l'échange d'informations, d'expériences, de connaissances, de bonne pratiques et d'accroître l'assistance technique et, dans certains cas, l'appui financier.

Il importe de créer des espaces de discussion et de s'employer à trouver des moyens efficaces de prévention, en appuyant le travail réalisé par l'ONU par l'entremise de ses organes compétents. Nous jugeons qu'il est également important de souligner que les infrastructures essentielles doivent être protégées

partout où elles se trouvent. L'Uruguay a parrainé la résolution 2286 (2016) sur la protection des hôpitaux et du personnel humanitaire dans les situations de conflit armé et attache une importance particulière à cette question.

En Amérique latine, certains pays se sont déjà dotés d'une stratégie et d'un cadre juridique en matière de sécurité cybernétique et de cyberdéfense et d'autres ont commencé à élaborer des politiques et des stratégies nationales intégrées en matière de sécurité cybernétique. En 2004, les États membres de l'Organisation des États américains (OEA) ont adopté à l'unanimité la Stratégie interaméricaine intégrée pour combattre les menaces à la sécurité cybernétique et en 2012, ils ont signé la Déclaration sur le renforcement de la sécurité cybernétique dans les Amériques. En outre, en 2015, le Comité interaméricain contre le terrorisme de l'OEA a adopté une déclaration sur la protection des infrastructures essentielles face aux menaces émergentes.

L'Uruguay s'est doté d'un centre national d'intervention face aux incidents de sécurité informatique, qui coordonne et exécute les interventions en cas d'incident et élabore et diffuse des normes en matière de politiques et les bonnes pratiques en vue de renforcer la sécurité. En collaboration avec l'organisme chargé de l'administration en ligne, l'Uruguay coopère avec d'autres pays et a établi des partenariats avec des organismes internationaux pour promouvoir la communication et la collaboration entre les centres d'intervention. C'est notamment le cas du Comité interaméricain contre le terrorisme et du Groupe de travail régional interorganisations sur les technologies de l'information et des communications. Il existe un département chargé des délits technologiques au niveau du Ministère de l'intérieur et en avril 2015, un centre d'intervention pour les incidents de sécurité cybernétique a été créé au sein du Ministère de la défense. Dans la première moitié de 2016, on a traité de 419 incidents liés à la sécurité informatique en Uruguay, ce qui représente une augmentation de 11 % par rapport à la même période l'an dernier. Entre autres facteurs, cette augmentation s'explique par les tendances mondiales en matière de cyberattaques et de cybercriminalité.

Il ne fait aucun doute que la capacité des États Membres de réagir aux attaques terroristes visant les infrastructures essentielles n'est pas la même, ce qui est dû en grande partie au fait qu'ils n'ont pas le même niveau de développement et les mêmes ressources. Par conséquent, nous devons être conscients de cette obligation collective de protéger, dans le plein respect de la souveraineté des États et en établissant le bon équilibre entre les mesures de sécurité et la protection des droits de l'homme et des libertés fondamentales.

M. Klein (États-Unis d'Amérique) (*parle en anglais*) : Je tiens à remercier tous les intervenants des exposés très instructifs et exhaustifs qu'ils ont faits aujourd'hui et d'avoir mis en relief le travail réalisé par leurs organisations relativement à cette question importante.

Les États-Unis remercient l'Ukraine d'avoir appelé l'attention sur l'importance qu'il y a à protéger les infrastructures essentielles. Le problème pour la plupart des gens est que les infrastructures essentielles se trouvent partout et nulle part. Nous ne pensons pas aux ponts et aux tunnels qui nous permettent de venir au travail tous les jours. Nous ne pensons pas aux radars, aux satellites et aux radios qui permettent aux avions de se déplacer en toute sécurité dans le ciel. Nous ne pensons pas aux réseaux des centrales électriques, des sous-stations et des lignes à haute tension qui font que les lumières sont toujours allumées. Nous ne pensons pas aux salles de serveurs et aux câbles à fibre optique qui permettent à nos courriels de parvenir à leurs destinataires. Par conséquent, lorsque nous parlons de la protection des infrastructures essentielles au Conseil de sécurité, nous parlons en fait de protéger les fondements de notre vie quotidienne à l'époque moderne.

Ce n'est pas un problème auquel on peut s'attaquer seul, et c'est pour cette raison que les États-Unis ont appuyé la résolution 2341 (2017) qui vient d'être adoptée par le Conseil. L'une des raisons est que les conséquences d'une attaque contre des infrastructures essentielles peuvent se faire sentir bien au-delà des frontières d'un pays donné. Les pipelines qui transportent le pétrole et le gaz – qui sont indispensables – s'étendent sur des milliers de kilomètres. Une catastrophe dans une usine chimique ou une centrale nucléaire pourrait provoquer des maladies à travers les continents. La liste est longue, mais le fait est que la protection des infrastructures essentielles peut nous aider tous à vivre en sécurité. Cependant, une autre raison pour laquelle nous devons coopérer est que les menaces contre les infrastructures essentielles peuvent être transnationales. Cela est particulièrement vrai s'agissant des menaces cybernétiques. En effet, des acteurs malveillants peuvent faire des ravages à travers les frontières. Nous pouvons dès lors convenir de l'importance de cette question et de ses dimensions

internationales. La question qui se pose maintenant est de savoir ce que les États Membres peuvent faire pour réduire le risque d’une attaque terroriste dévastatrice.

Aux États-Unis, la majorité des infrastructures essentielles appartiennent à des entreprises privées, raison pour laquelle leur protection est une responsabilité partagée entre le Gouvernement, les entreprises et les particuliers, à différents niveaux. Il s’agit d’un effort de collaboration. En fait, quiconque dans cette salle a pris le métro à New York a certainement vu les nombreux panneaux qui rappellent aux passagers : « Si vous voyez quelque chose, dites quelque chose ». Cela fait partie de la stratégie. Tout acte supplémentaire de vigilance est de mise. Le Gouvernement des États-Unis, plus particulièrement le Département de la sécurité du territoire, travaille constamment à des partenariats public-privé qui renforcent la résilience de nos communautés. Les États-Unis pensent que les organismes et les institutions des Nations Unies chargés de lutter contre le terrorisme peuvent s’avérer utiles. Ils peuvent recueillir l’information sur la façon dont les États Membres peuvent traiter les infrastructures essentielles et mettre en commun les pratiques optimales pour protéger ces institutions.

La résolution d’aujourd’hui rappelle aussi que les États Membres de l’ONU doivent veiller à ériger les actes de terrorisme en infractions graves, notamment ceux visant à détruire les infrastructures essentielles ou à les rendre inutilisables. Cela est important en partie pour dissuader, mais aussi pour s’assurer que les auteurs de ces attaques n’échappent pas aux poursuites. Les États Membres doivent renforcer les partenariats afin de mettre en commun l’information sur les menaces potentielles et veiller à ce que leurs services de répression et autres entités concernées puissent œuvrer de concert pour prévenir les attaques avant qu’elles n’aient lieu. Comme le Ministre l’a dit, un homme averti en veut deux.

Il s’agit d’un nouveau domaine de coopération dont le Conseil doit débattre, et il nous reste donc beaucoup à faire, notamment pour définir le rôle des Nations Unies s’agissant d’aider les États Membres à coopérer. Mais la résolution adoptée aujourd’hui doit insuffler une dynamique afin de donner concrètement les moyens aux gouvernements de mettre en commun les enseignements tirés et de collaborer pour faire que les infrastructures essentielles continuent de fonctionner en toute sécurité à l’arrière-plan de notre vie quotidienne, comme elles le doivent.

M. Aboulatta (Égypte) (*parle en arabe*) : Je voudrais tout d’abord vous remercier, Monsieur le Président, et féliciter sincèrement le Conseil de sécurité d’avoir adopté l’importante résolution 2341 (2017) sur la protection des infrastructures essentielles contre les attaques terroristes. Je remercie aussi la présidence ukrainienne du Conseil de sécurité d’avoir organisé ce débat important. Et je remercie les différents orateurs de leurs exposés pénétrants.

Les actes terroristes dont est témoin le monde aujourd’hui confirment que la protection des infrastructures essentielles est primordiale et qu’elle doit avoir la priorité dans le cadre de nos efforts visant à lutter contre le terrorisme, en particulier du fait du nombre croissant de victimes d’attaques terroristes ciblant les infrastructures essentielles et de leurs conséquences négatives sur un grand nombre de peuples de la planète où surviennent ces attaques, et dont les répercussions s’étendent parfois à d’autres pays.

La résolution qui vient d’être adoptée aujourd’hui est la première du genre à porter sur la question de la protection des infrastructures essentielles contre les attaques terroristes. Elle soulève de nombreux points importants qu’il faut prendre en considération, notamment que chaque État doit déterminer quelles sont ses infrastructures essentielles, surtout en l’absence de définition internationale précise à cet égard, ainsi que les moyens de les protéger efficacement contre toute attaque terroriste. Elle engage aussi tous les États à se coordonner entre eux, à renforcer la coopération internationale, à mettre en commun les informations et à mener des activités de sensibilisation, de façon à être mieux préparés en cas d’attaque contre des infrastructures essentielles. Elle demande aussi aux États Membres d’envisager d’élaborer des stratégies de réduction des risques posés par les attaques terroristes au regard des infrastructures essentielles. Elle demande instamment aux États qui sont en mesure de le faire de fournir l’assistance nécessaire pour renforcer les capacités des États et leur permettre de protéger les infrastructures essentielles contre les attaques terroristes, que ce soit par la formation, la fourniture d’autres ressources et services techniques nécessaires, et le transfert de technologie.

L’adoption par le Conseil de sécurité de la résolution sur la protection des infrastructures essentielles contre les attaques terroristes est une mesure importante. Mais ce qui est plus important, c’est de mettre en œuvre cette résolution et d’autres résolutions du Conseil de sécurité

concernant la lutte contre le terrorisme. Cela requiert du Conseil qu’il assure un suivi de tous les instants et qu’il demande des comptes aux pays et aux régimes qui ne mettent pas pleinement en œuvre ces résolutions, ainsi qu’à ceux qui continuent d’appuyer le terrorisme, de le financer, d’accorder asile aux terroristes et de les approvisionner en armes. Ces pays et régimes sapent nos efforts et font fi des résolutions du Conseil de sécurité visant à neutraliser et à éliminer le terrorisme. Le moment est venu pour eux de répondre de leur appui au terrorisme.

Pour terminer, je voudrais remercier encore une fois la présidence ukrainienne du Conseil de sécurité et réaffirmer que l’Égypte est déterminée à rester à la pointe de l’action menée par la communauté internationale pour vaincre le terrorisme, dans le respect du droit international, de l’état de droit et des droits de l’homme.

M. Rycroft (Royaume-Uni) (*parle en anglais*) : Je suis extrêmement reconnaissant des analyses faites par les personnalités qui ont présenté des exposés ce matin. Je me joins aux autres intervenants pour vous féliciter, Monsieur le Ministre, du leadership dont vous avez fait preuve s’agissant de porter cette importante question à notre attention.

La menace terroriste a évolué au fil des décennies. Nous faisons face à des menaces de plus en plus complexes à mesure que les terroristes acquièrent de nouvelles connaissances et de nouvelles technologies. Ne se contentant pas de simplement tuer des innocents, les terroristes cherchent à nous déstabiliser, à nous démoraliser et à perturber notre mode de vie. Les infrastructures essentielles, qu’il s’agisse d’un système de transport, d’un nœud de communications ou d’un réseau électrique, représentent un cible attirante pour ces sinistres acteurs. Le fait que les auteurs des attaques contre le métro et l’aéroport de Bruxelles en mars dernier aient aussi consacré du temps à la surveillance d’un scientifique nucléaire belge doit nous préoccuper tous. Nous devons redoubler de vigilance pour veiller à être préparés à défendre les systèmes qui permettent à nos sociétés de fonctionner.

C’est pourquoi nous nous félicitons sincèrement de la mesure prise aujourd’hui par le Conseil de sécurité d’adopter la résolution 2341 (2017). La résolution place cette importante question sur le devant de la scène, demande aux États d’améliorer leur état de préparation et de renforcer notre coopération aux fins de la protection de la sécurité de nos populations et de nos infrastructures essentielles. Si nous voulons vraiment contrer cette menace, je crois que nous devons nous axer sur trois choses, à savoir la préparation, la protection et les partenariats.

Premièrement, s’agissant de la préparation, il est fondamental que les plans visant à protéger nos infrastructures essentielles soient élaborés, maintenus et testés de façon globale. Nous faisons écho à la demande faite par la résolution aux États d’élaborer leurs propres stratégies pour se préparer et répondre à toute attaque. Les menaces contre nos infrastructures peuvent émaner de plusieurs sources : le terrorisme, la criminalité ou les catastrophes naturelles. S’agissant de réduire le risque encouru par nos infrastructures, le Royaume-Uni adopte une démarche qui tient compte de l’ensemble des menaces. Cela signifie élaborer des plans qui peuvent être utilisés pour répondre à tous les types de perturbation ou menaces à la vie. Les mesures prises par les États pour prévenir l’ingérence illégale ou criminelle dans la gestion de nos infrastructures peuvent aussi aider à prévenir les attaques terroristes. C’est, pour une part, grâce aux mesures fermes que nous avons prises que les menaces terroristes contre nos infrastructures sont atténuées.

Deuxièmement, en ce qui concerne la protection, la menace contre certains éléments de nos infrastructures essentielles peut être considérée comme démesurée, mais s’il y a un secteur où la menace est très réelle et le risque très élevé, c’est celui du transport. Comme les derniers rapports du Secrétaire général le montrent, le terrorisme international continue de faire peser une menace grave et persistante sur nos réseaux de transport, en particulier l’aviation civile. Trois milliards de passagers atteignent leur destination par voie aérienne chaque année. L’année dernière ne nous a que trop souvent rappelé les risques auxquels nous faisons face : les attaques contre les aéroports de Bruxelles et d’Istanbul, la destruction de l’appareil de la compagnie russe Metrojet au-dessus du Sinaï, et l’explosion à bord d’un vol de Daallo Airlines en provenance de Mogadiscio. C’est pour lutter contre ces menaces que le Royaume-Uni a présenté la résolution 2309 (2016), et c’est pourquoi nous faisons écho aujourd’hui à notre appel lancé eux États leur demandant de coopérer avec l’Organisation de l’aviation civile internationale. En œuvrant de concert, nous pouvons faire non seulement que les normes internationales de sécurité ne restent pas en deçà de la menace terroriste, mais aussi – et c’est indispensable – qu’elle soient effectivement appliquées sur le terrain.

Enfin, concernant les partenariats, les infrastructures essentielles que nous devons protéger sont pour une grande part la propriété du secteur privé, et peuvent aussi être partie intégrante de réseaux internationaux et de chaînes d’approvisionnement complexes. La préparation et la protection des infrastructures ne resteront que des vœux pieux si nous échouons à œuvrer dans tous les secteurs pour les concrétiser. Chaque partie à un rôle à jouer. Les sociétés privées ont la responsabilité de veiller à ce que leurs infrastructures sont protégées et que les services essentiels fonctionnent, tout comme les gouvernements ont l’obligation d’assurer que le secteur concerné gère ces risques pleinement et de façon responsable. Comme la résolution d’aujourd’hui l’indique, des partenariats internationaux solides sont essentiels à l’heure où le fonctionnement des infrastructures dépend de réseaux et de chaînes d’approvisionnement transfrontières. Le partage de l’information, des réseaux d’alerte précoce et des compétences permettra de renforcer notre approche commune.

Le Conseil de sécurité doit rester informé de l’évolution de la menace terroriste et y faire face. De même que nous agissons pour prévenir les conflits, nous devons agir de façon préventive pour empêcher le terrorisme. Aujourd’hui, nous avons ajouté une nouvelle pierre qui permettra de renforcer nos efforts communs. Grâce à nos efforts, les terroristes décidés à déclencher le chaos ont un autre obstacle à franchir. Grâce à nos efforts, nos sociétés sont peu plus sûres qu’elles ne l’étaient hier.

M. Liu Jieyi (Chine) (*parle en chinois*) : La Chine remercie l’Ukraine d’avoir organisé le présent débat public sur la protection des infrastructures essentielles contre les attaques terroristes. Nous souhaitons la bienvenue au Ministre des affaires étrangères, M. Klimkin, qui préside la séance. Nous avons écouté attentivement les exposés faits par la Directrice de cabinet du Secrétaire général, Mme Viotti, et les autres intervenants.

Alors que la mondialisation économique s’intensifie et que l’interconnexion des pays augmente, les infrastructures sont d’une très grande importance pour le développement des économies et le renforcement de l’interconnectivité et de l’intégration économique. Toutefois, s’agissant de la lutte contre le terrorisme, la situation ne cesse de s’aggraver et les infrastructures sont de plus en plus une cible facile pour les attaques terroristes. Récemment, une série d’attentats terroristes contre des infrastructures, tels que des aéroports et des stations de transports publics, ont semé la panique et causé de graves pertes humaines et matérielles. La communauté internationale doit suivre de près l’évolution de la situation et œuvrer de concert pour lutter contre ce phénomène.

Premièrement, les pays doivent s’employer à assurer la sécurité des projets d’interconnexion régionale et d’autres infrastructures essentielles. La collaboration régionale a une incidence considérable sur le développement économique et la prospérité à l’échelle mondiale. L’initiative chinoise « Une Ceinture et une Route » a fait de l’interconnexion des infrastructures l’une de ses priorité, l’objectif étant de soutenir les pays le long de la Route en contribuant au développement de leurs infrastructures, en instaurant une coopération mutuellement bénéfique et en synchronisant le développement au profit de tous. À ce jour, plus d’une centaine de pays et organisations internationales se sont joints à cette initiative. La Chine espère renforcer la coopération dans des domaines, tels que le partage de renseignements, l’évaluation des risques et la conduite d’activités conjointes de maintien de l’ordre, tant bilatéralement que multilatéralement, conformément aux résolutions pertinentes du Conseil de sécurité et de l’Assemblée générale, afin de protéger efficacement les projets d’interconnexion et les infrastructures transfrontières contre les attaques terroristes et d’assurer la sécurité des ouvrages construits dans le cadre de l’initiative.

Deuxièmement, les pays doivent assumer la responsabilité principale de la protection de leurs infrastructures. Conformément aux exigences stipulées dans la résolution 2341 (2017), la Chine espère qu’ils renforceront leur coordination et élaboreront des politiques de sécurité nationales en tenant compte des risques d’attaques terroristes. Ils devront notamment renforcer leur capacité à protéger les infrastructures contre ces attaques grâce à la surveillance, aux systèmes d’alerte rapide et aux mesures d’urgence, afin d’assurer leur sûreté et leur sécurité.

Troisièmement, les pays doivent renforcer la coopération internationale dans le domaine de la sécurité des infrastructures, et ce, de manière globale en vue d’édifier une communauté humaine au destin partagé. Les pays développés doivent aider les pays en développement à renforcer leurs capacités dans ce domaine. Les parties doivent accroître leur coopération en matière d’échange d’informations, d’application

des lois et d'entraide judiciaire afin de lutter contre les attaques terroristes visant les infrastructures. Les organisations internationales et régionales concernées doivent aider les États Membres à mettre en commun les meilleures pratiques et à renforcer les capacités nationales en matière de prévention. L'ONU et le Conseil de sécurité doivent jouer un rôle de premier plan dans la coopération internationale dans ce domaine.

Le terrorisme est l'ennemi commun de l'ensemble de l'humanité. Quels que soient le moment et le lieu où il frappe et quelle qu'en soit la forme, il doit être combattu avec détermination. Les pays doivent respecter des normes uniformes et lutter farouchement contre toutes les organisations terroristes qui figurent sur la liste du Conseil de sécurité. Les mesures internationales de lutte contre le terrorisme doivent maximiser le rôle de chef de file de l'ONU et du Conseil de sécurité et respecter les buts et principes énoncés dans la Charte des Nations Unies afin d'assurer une coordination efficace. En tant que membre important du camp international de la lutte contre le terrorisme, la Chine poursuivra sa coopération bilatérale et multilatérale conformément à sa législation nationale en matière de lutte contre le terrorisme et aux conventions internationales pertinentes afin d'assurer de manière efficace la protection et la sécurité des infrastructures et de collaborer avec la communauté internationale en vue de lutter contre le terrorisme et de préserver la paix, la sécurité et la stabilité internationales.

M. Zagaynov (Fédération de Russie) (*parle en russe*) : Je voudrais moi aussi remercier les intervenants de leur participation à la séance d'aujourd'hui.

La lutte contre le terrorisme dans le monde d'aujourd'hui doit être une priorité absolue des travaux du Conseil de sécurité. Aujourd'hui, la communauté internationale fait face à des formes de plus en plus sophistiquées d'activités terroristes et de l'appui qui leur est fourni. L'État islamique d'Iraq et du Levant (EIIL), le Front el-Nosra, Al-Qaida et leurs alliés s'adaptent à l'évolution de la situation, introduisant de nouvelles formes de financement et utilisant avec habileté les technologies modernes de l'information pour développer leur base matérielle et attirer des recrues. Le Conseil de sécurité doit faire tout ce qui est en son pouvoir pour parer à ces nouvelles menaces.

Guidée par ces principes, notre délégation a présenté plusieurs initiatives au sein du Conseil de sécurité. Aux fins de la mise en œuvre de nombre de ces initiatives, nous nous sommes appuyés sur les structures antiterroristes de l'ONU et des États Membres, et notamment sur une série de mesures visant à tarir les ressources financières du terrorisme telles qu'énoncées dans la résolution 2199 (2015). En outre, des mesures importantes pour lutter contre l'EIIL et son financement sont envisagées dans la résolution 2253 (2015), qui a été proposée par la Russie et les États-Unis.

Un certain nombre de menaces terroristes demeurent aujourd'hui sans réponse adéquate. Coordonner les efforts déployés par les membres de la communauté internationale dans ce domaine contribuerait à la mise en place de la vaste coalition internationale contre le terrorisme qui a été proposée par la Fédération de Russie. Nous avons présenté au Conseil de sécurité un projet de résolution sur la lutte contre l'idéologie terroriste qui met l'accent sur sa propagation par le biais d'Internet. Ces approches bénéficient de l'appui de nombreux membres du Conseil de sécurité. Par ailleurs, notre délégation continue d'appuyer les propositions qui visent à trouver les moyens les plus efficaces de lutter contre les défis actuels du terrorisme.

Dans le même temps, nous pensons que lorsque le Conseil de sécurité prépare de nouvelles décisions, en particulier dans un domaine aussi important que la lutte contre le terrorisme, l'accent doit être mis sur les questions vraiment importantes, en prêtant une attention particulière à la valeur ajoutée et à l'obtention de résultats concrets. Il ne vaut pas la peine d'entamer des négociations pour simplement décrire des points évidents ou reproduire des déclarations qui ont été utilisées à de nombreuses reprises dans d'autres documents nationaux ou internationaux. Bien entendu, il n'y a aucun mal à vouloir poursuivre une telle approche, mais elle n'a jamais donné de résultat tangible.

Nous voudrions une fois de plus appeler les membres du Conseil à œuvrer résolument et de manière coordonnée pour élaborer des réponses efficaces et communes aux défis pernicieux du terrorisme, défis qui viennent, avant tout, de l'EIIL, du Front el-Nosra et d'Al-Qaida et des groupes qui leur sont affiliés. La gravité de ces menaces n'a pas diminué.

M. Arancibia Fernández (État plurinational de Bolivie) (*parle en espagnol*) : Tout d'abord, je voudrais souhaiter la bienvenue au Ministre des affaires étrangères, M. Klimkin, et féliciter, par son intermédiaire, la délégation ukrainienne d'avoir inscrit cette question à l'ordre du jour du Conseil de sécurité. Je souhaiterais féliciter et remercier tous les intervenants qui m'ont précédé.

L'État plurinational de Bolivie réaffirme son ferme attachement à la lutte contre le terrorisme, ainsi que sa condamnation catégorique des actes terroristes, quels qu'en soient les motifs et les auteurs et où qu'ils soient commis, étant donné qu'ils portent délibérément atteinte à la paix et à la sécurité internationales et constituent des violations flagrantes du droit international. Dans le même temps, nous rappelons que ce fléau ne saurait être associé à une religion, une nationalité, une civilisation ou un groupe ethnique en particulier.

L'objectif du présent débat est d'encourager les États Membres à évaluer les facteurs de vulnérabilité, les relations d'interdépendance et leurs capacités de protection des infrastructures essentielles, ainsi que les effets en cascade que provoqueraient des attaques terroristes visant ces infrastructures. De même, ils sont également invités à envisager d'éventuelles mesures préventives lors de l'élaboration de leurs stratégies et politiques nationales. Notre délégation a participé aux négociations sur la résolution 2341 (2017) sur la protection des infrastructures essentielles contre les attaques terroristes qui a été adoptée aujourd'hui, et nous voudrions mettre en avant plusieurs de ses éléments.

Nous rappelons tout d'abord les résolutions que le Conseil de sécurité a adoptées en réponse à la grave menace mondiale que représente le terrorisme depuis la résolution 1373 (2001). Il y réaffirme son respect pour la souveraineté, l'intégrité territoriale et l'indépendance politique de tous les États, conformément à la Charte des Nations Unies. Nous soulignons ensuite l'importance de mettre en œuvre la Stratégie antiterroriste mondiale des Nations Unies, approuvée par la résolution 60/288 de l'Assemblée générale en date du 8 septembre 2006, dans laquelle est réaffirmée la nécessité de prendre des mesures pour prévenir et combattre le terrorisme. Nous insistons en particulier sur le deuxième pilier de la Stratégie, qui souligne la nécessité de renforcer les efforts visant à améliorer la sécurité et la protection des cibles particulièrement vulnérables comme les infrastructures et les lieux publics.

Dans le même temps, nous reconnaissons qu'il revient à chaque État de déterminer quelles sont ses infrastructures essentielles et la manière de les protéger efficacement contre les attaques terroristes. Nous estimons en outre que c'est aux États qu'il incombe au premier chef de riposter aux attaques terroristes contre ce qu'ils considèrent être leurs infrastructures essentielles, qu'elles soient publiques ou privées, le tout dans le respect de la législation nationale. Nous appuyons les efforts du Comité contre le terrorisme, avec l'appui de la Direction exécutive, pour poursuivre son travail en faveur de la mise en œuvre de la résolution 1373 (2001), notamment en ce qui concerne l'assistance aux États Membres et la protection des infrastructures essentielles contre les attaques terroristes afin de recenser les pratiques optimales, ainsi que les lacunes et les vulnérabilités dans ce domaine. À cet égard, nous invitons le Comité contre le terrorisme à continuer d'œuvrer avec l'Équipe spéciale de lutte contre le terrorisme pour faciliter l'assistance technique et le renforcement des capacités et susciter une prise de conscience en matière de protection des infrastructures essentielles contre les attaques terroristes, notamment grâce au renforcement du dialogue avec les organisations régionales et sous-régionales compétentes qui travaillent en contact étroit les unes avec les autres, en s'appuyant tout particulièrement pour ce faire sur l'échange d'information.

Le dispositif juridique relatif au problème du terrorisme s'est développé à mesure que se sont multipliés les actes terroristes dans les diverses régions du monde. Il importe de reconnaître les efforts déployés par les gouvernements et les peuples pour lutter contre ce fléau.

Enfin, nous considérons qu'il est important que les États assument leurs responsabilités en ce qui concerne la lutte contre le terrorisme, et protègent notamment les infrastructures essentielles en appliquant pleinement les dispositions à cet effet qui figurent dans les instruments internationaux et les résolutions pertinentes de cet organe multilatéral qu'est le Conseil, de même qu'en mettant concrètement en oeuvre la Stratégie antiterroriste mondiale des Nations Unies.

Le Président (*parle en anglais*) : Je rappelle à tous les orateurs qu'ils sont priés de limiter la durée de leurs déclarations à un maximum de cinq minutes afin que le Conseil puisse mener ses travaux avec diligence.

Les délégations qui ont préparé de longues déclarations sont priées de bien vouloir en distribuer le texte et d'en lire une version abrégée lorsqu'elles prendront la parole dans la salle.

Je donne maintenant la parole au Ministre des affaires étrangères de l'Estonie.

M. Mikser (Estonie) (*parle en anglais*) : Je voudrais commencer par remercier l'Ukraine d'avoir organisé ce débat très opportun aujourd'hui.

L'Estonie s'associe à la déclaration qui sera faite par l'observateur de l'Union européenne. Nous nous sommes également portés coauteurs de la résolution 2341 (2017), sur la protection des infrastructures essentielles contre les attaques terroristes.

Notre objectif à tous est de nous assurer que la sécurité n'est pas un luxe, mais un élément essentiel à la disposition de tous. Bien que la menace terroriste en Estonie demeure faible, nous avons été profondément touchés par les actes de terrorisme commis dans notre région et au-delà, et il continuera d'en être ainsi. L'Estonie reste donc très attachée aux efforts conjoints que nous déployons pour lutter contre le terrorisme.

Le terrorisme est un phénomène de plus en plus inquiétant, tant par son ampleur que par sa géographie. L'année dernière, nous avons été témoins d'une série d'actes de terreur effroyables commis un peu partout dans le monde, y compris dans notre région, l'Europe. Plusieurs de ces attaques ont visé des infrastructures essentielles. Nous avons encore tous en mémoire les attentats odieux commis contre les aéroports de Bruxelles et d'Istanbul, dans lesquels de nombreux innocents ont perdu la vie. De fait, les infrastructures essentielles, comme les banques, les télécommunications, les systèmes d'approvisionnement en eau ou en énergie, les transports et les services d'urgence, sont des cibles de choix pour les terroristes. La vulnérabilité des infrastructures essentielles est exacerbée par la dépendance de plus en plus grande à l'égard des technologies de l'information et des communications dans un monde toujours plus interconnecté. Les attaques contre ces infrastructures, y compris les cyberattaques, peuvent donc provoquer de graves dégâts et de lourdes pertes en vies humaines.

L'Estonie sait ce qu'être la cible d'une cyberattaque à grande échelle veut dire. En 2007, notre degré de préparation et la rapidité avec laquelle nous avons réagi ont empêché que notre infrastructure soit gravement endommagée. Toutefois, les cyberattaques qui ont visé l'Estonie cette année-là ont clairement montré l'importance de considérer la cybersécurité comme un élément à part entière de notre dispositif de sécurité nationale.

Un des maîtres-mots pour lutter contre cette menace est la résilience. En ce qui concerne les infrastructures essentielles, la résilience suppose la participation étroite du secteur privé, qui souvent est le propriétaire et l'opérateur de ces services vitaux. Dans certains domaines, comme la banque, la cybersécurité est devenue partie intégrante du fonctionnement, mais la cybersécurité devrait susciter le même degré de priorité dans d'autres secteurs également. Nous devons aussi comprendre, en tant que gouvernements, que le partage de l'information ne saurait être une voie à sens unique, qui irait des entreprises vers le gouvernement. Afin de renforcer la confiance, d'améliorer la sécurité et de partager les pratiques optimales ainsi que l'information sur les vecteurs de menace potentiels, les gouvernements doivent aussi partager les informations dont ils disposent avec le secteur privé.

Outre la coopération entre le secteur privé et le secteur public, la société civile joue un rôle extrêmement important dans le renforcement de la confiance. Pour véritablement rendre les sociétés plus fortes, les gouvernements doivent informer les citoyens des menaces potentielles qui pèsent sur les infrastructures essentielles et veiller à ce qu'ils soient prêts à faire face aux conséquences d'une éventuelle attaque. Un des grands éléments qui a contribué à ce que nous puissions faire face aux cyberattaques de 2007 a été la coopération horizontale entre les experts en sécurité informatique. Cette expérience a conduit à la création de l'unité de cyberdéfense au sein des forces de défense paramilitaires estoniennes, un modèle novateur permettant à des volontaires de participer à la cyberdéfense nationale.

Il est primordial que les pays établissent la liste de leurs infrastructures essentielles et de leurs dépendances transfrontières afin d'améliorer la cybersécurité et la résilience au niveau national. Aucun pays ne peut faire face seul à tout l'éventail des cybermenaces et la coopération internationale est fondamentale pour prévenir les scénarios catastrophes. Nous encourageons par conséquent les pays à partager davantage leurs connaissances et à contribuer au renforcement des capacités au-delà de leurs frontières, afin de favoriser ainsi une plus grande prise en compte des menaces à la cybersécurité et une meilleure atténuation de leurs effets.

L'Estonie dispose d'une vaste expérience s'agissant de mener ou seconder divers efforts de renforcement des capacités en matière de cybersécurité et de développement numérique à travers le monde. Nous allons continuer de partager nos meilleures pratiques et les enseignements tirés de notre expérience. Ici à l'ONU, nous sommes fiers de concourir à la cybersécurité par l'entremise du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale.

Une coopération globale est le fondement de la résilience. Elle garantit que les acteurs critiques de la cybersécurité – les gouvernements, les forces armées, les services de renseignement, les exploitants d'infrastructures critiques et les acteurs clefs du secteur privé – soient pleinement informés, préparés et capables de traiter des cyberattaques à grande échelle.

Je voudrais rappeler l'importance de la Convention de Budapest sur la cybercriminalité. Elle est le seul instrument international contraignant traitant de la cybercriminalité et porte également sur l'utilisation d'Internet à des fins terroristes. La mise en œuvre effective de la Convention sur la cybercriminalité garantirait que les législations nationales prévoient des sanctions appropriées pour les cas d'attaques graves, y compris les actes de terrorisme, contre les infrastructures basées sur la technologie de l'information ou contre les infrastructures informatiques en général.

L'Estonie appelle tous les pays à adopter des politiques, des stratégies et des règlements qui contribuent à créer et à maintenir un cyberespace ouvert, résilient, sûr et pacifique. Nous devons respecter les plus hautes normes de diligence raisonnable dans le développement et l'utilisation des technologies de l'information et des communications.

La prévention est le seul moyen d'empêcher complètement la radicalisation et le recrutement dans les organisations terroristes, ainsi que d'éliminer la menace terroriste contre les infrastructures essentielles. Nous appuyons le Plan d'action du Secrétaire général pour la prévention de l'extrémisme violent. Dans tous les pays, la priorité la plus haute doit être accordée à la prévention de futures menaces.

Dans ce contexte, je voudrais saluer l'initiative du Secrétaire général visant à consolider et à rationaliser les mécanismes antiterroristes de l'Organisation des Nations Unies tout en améliorant leur transparence. Nous espérons que la nouvelle structure aura également pour objectif principal la prévention de l'extrémisme violent.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de la Slovaquie.

M. Ružička (Slovaquie) (*parle en anglais*) : Je vous remercie, Monsieur le Président, de tenir ce débat sur la protection des infrastructures essentielles contre les attaques terroristes et de promouvoir une discussion sur les mesures préventives contre de telles attaques. Dans ce contexte, je voudrais rappeler les résultats de la réunion tenue selon la formule Arria sur la cybersécurité et la paix et la sécurité internationales organisée par l'Espagne et le Sénégal en novembre 2016.

À mesure que l'horizon des menaces change et devient plus complexe, notre approche des problèmes de sécurité doit également évoluer face aux menaces asymétriques et transfrontalières. De ce fait, elles doivent être confrontées aux niveaux national et international. Aucun pays n'est à l'abri des menaces du cyberterrorisme, y compris le mien. La Slovaquie a adopté une stratégie nationale de lutte contre le terrorisme, fondée sur quatre grands piliers, conformément aux objectifs du plan d'action de l'Union européenne en matière de lutte contre le terrorisme : prévention, protection, poursuites et riposte.

Les menaces posées par des perturbations majeures des infrastructures essentielles à l'économie, à l'infrastructure et à la sécurité nationale d'un pays sont réelles. Ces menaces peuvent être classées en trois catégories : les menaces naturelles, humaines et accidentelles ou techniques.

Bien que la réduction des vulnérabilités des infrastructures critiques et l'accroissement de leur résilience relèvent de la responsabilité de chaque État, la nécessité d'une coopération internationale croît rapidement. Comme cela a été mentionné, les cybermenaces et les attaques deviennent de plus en plus fréquentes et sophistiquées et nuisent aux États, car nous dépendons de plus en plus des systèmes de communication informatiques. Actuellement, les attaques cyberterroristes sont généralement considérées comme présentant un risque relativement faible pour les États. Mais bien que les cyberattaques se produisent avec plus de fréquence et d'intensité dans le monde entier, beaucoup ne sont pas signalées ou sont sous-déclarées, laissant au public un faux sentiment de sécurité à propos de la menace elle-même.

Alors que les gouvernements, les entreprises et les individus sont tous ciblés sur une base exponentielle, l'infrastructure devient une cible de choix parmi les cyberattaqueurs individuels et ceux qui sont parrainés par des États, qui reconnaissent la valeur de perturber ce qui était auparavant considéré comme des systèmes de sécurité impénétrables. Beaucoup de pays autour de cette table ont déjà eu à faire face à ce genre d'actions récemment. Selon le rapport annuel de sécurité de Dell pour l'année 2015, les cyberattaques contre les systèmes de contrôle et d'acquisition de données ont doublé en 2014, se chiffrant à plus de 160 000.

Aujourd’hui, selon INTERPOL, les codes malveillants peuvent être utilisés pour manipuler les contrôles des réseaux électriques, des services financiers, des fournisseurs d’énergie, des systèmes de défense, des bases de données sur les soins de santé et d’autres infrastructures essentielles, entraînant des dommages physiques catastrophiques dans le monde réel, tels que des pannes d’électricité, ou la perturbation de l’approvisionnement en eau d’une ville entière.

Notre action commune est nécessaire. Certaines études suggèrent que les mesures suivantes devraient être prises pour améliorer la protection des infrastructures essentielles : premièrement, évaluer les vulnérabilités de ces infrastructures; deuxièmement, élaborer des plans pour éliminer les vulnérabilités importantes; troisièmement, proposer des systèmes permettant d’identifier et de prévenir les tentatives d’attaques majeures; quatrièmement, élaborer des plans pour alerter, contenir et repousser les attaques en cours; et cinquièmement, reconstituer rapidement les capacités essentielles minimales après une attaque.

On ne saurait exclure qu’à l’avenir, l’utilisation du cyberespace par des acteurs étatiques ou non étatiques pourrait constituer une menace pour la paix et la sécurité internationales et exigerait du Conseil de sécurité qu’il prenne des mesures plus décisives pour y répondre.

Comme l’a déclaré le Secrétaire général dans l’avant-propos du rapport de 2015 (A/70/174) du Groupe d’experts gouvernementaux chargé d’examiner les progrès de l’informatique et des télécommunications dans le contexte de la sécurité internationale en 2015 :

> « Seule la coopération internationale permettra de rendre le cyberespace stable et cette coopération doit reposer sur le droit international et sur les principes de la Charte des Nations Unies. »

Malheureusement, les traités internationaux visant à remédier au problème ont eu jusqu’à présent un impact limité en raison, d’une part, de l’incapacité à forcer les signataires à rendre compte de leurs actes et, d’autre part, de la difficulté de déterminer avec précision l’identité des acteurs responsables.

Un meilleur partage de l’information, conjugué à un mandat axé sur la diffusion rapide et précise des informations concernant les attaques contre les citoyens touchés, constitue une base solide pour la conception d’un protocole permettant de traiter efficacement les attaques futures et pourrait s’avérer utile, mais très peu de gouvernements s’engagent régulièrement dans cette pratique.

La Stratégie antiterroriste mondiale des Nations Unies invite les États Membres à améliorer les efforts visant à assurer la sécurité et la protection des cibles particulièrement vulnérables et à partager les meilleures pratiques, et souligne l’importance de développer des partenariats public-privé dans ce domaine. Mais encore une fois, dans la pratique, très peu à été fait, comme en témoigne l’expérience de nombreux pays.

À cet égard, je voudrais souligner les cinq points suivants sur lesquels nous devrions nous concentrer.

Il est nécessaire, premièrement, d’aider les États à apporter une aide concrète à la mise en œuvre des dispositions de la Stratégie antiterroriste mondiale des Nations Unies; deuxièmement, d’établir des mécanismes appropriés pour faciliter le partage accru des meilleures pratiques; troisièmement, de renforcer les capacités des secteurs public et privé et d’accroître le développement des partenariats public-privés, notamment en favorisant la prise de conscience et la compréhension de l’équilibre nécessaire entre les intérêts économiques et de sécurité afin d’assurer un niveau adéquat de protection et de limiter les effets préjudiciables des perturbations sur la société et les citoyens; quatrièmement, d’être plus décisif dans les efforts de lutte contre le blanchiment d’argent et le financement du terrorisme, car c’est par cette voie que beaucoup de savoir-faire tombe entre de mauvaises mains; et cinquièmement, que le Conseil de sécurité envisage de mieux utiliser le Groupe de travail sur la protection des infrastructures critiques, y compris Internet, les cibles vulnérables et la sécurité du tourisme de l’Équipe spéciale de lutte contre le terrorisme. Tout cela devrait viser à éviter, à traiter et à prévenir les attaques contre des infrastructures essentielles telles que celles qui ont eu lieu ces dernières décennies dans de nombreux pays représentés dans cette salles et contre d’autres Membres des Nations Unies.

Le terrorisme constitue une menace non seulement pour notre sécurité, mais aussi pour les valeurs, les droits et les libertés de nos sociétés et de leurs citoyens. Mon pays est déterminé à jouer son rôle dans les efforts régionaux et mondiaux de lutte contre le terrorisme et l’extrémisme violent sur tous les fronts, y compris la protection des infrastructures essentielles et le partage des meilleures pratiques et technologies.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant du Pérou.

M. Meza-Cuadra (Pérou) (*parle en espagnol*) : Je voudrais tout d’abord remercier la présidence ukrainienne d’avoir convoqué ce débat public du Conseil de sécurité sur la question de la protection des infrastructures essentielles contre les attaques terroristes, et saluer tout particulièrement M. Pavlo Klimkin, Ministre des affaires étrangères de l’Ukraine, qui nous honore de sa présence aujourd’hui. Nous remercions également les orateurs précédents et nous félicitons de l’adoption de la résolution 2341 (2017).

La protection des infrastructures essentielles, en particulier contre les attaques de groupes terroristes, doit être une priorité pour tous les États dans le cadre de la Stratégie antiterroriste mondiale des Nations Unies, en vue de préserver la santé, la sécurité et le bien-être économique des citoyens, ainsi que le bon fonctionnement de l’État et de son administration.

Comme cela a été signalé, les infrastructures essentielles comprennent les diverses installations, réseaux et services de la structure économique et sociale des États, y compris les voies de communication, les services de base et les installations touristiques et récréatives. Celles-ci doivent être prises en compte dans le processus de conception des stratégies de protection.

Le Pérou ayant été victime, dans le passé, du fléau du terrorisme, nous savons que les infrastructures essentielles sont une cible de choix pour les organisations terroristes, du fait de leurs vulnérabilités, d’autant plus que les attaques contre les infrastructures essentielles ont de graves conséquences, telles que la perte de vies humaines et la destruction de biens, ainsi que, à moyen et à long terme, des pertes économiques et l’insécurité au sein de la population.

De même, avec le développement des technologies de l’information et des communications, les infrastructures virtuelles et Internet sont également devenus des cibles pour les attaques de ce type d’organisations. Les interconnexions croissantes et une dépendance accrue à l’égard des technologies augmentent notre vulnérabilité. Les services d’une tour de contrôle d’aéroport, une centrale nucléaire et les valves d’un barrage peuvent être attaqués simultanément à distance.

Au Pérou, conscients de l’importance de se protéger face à ces menaces, nous avons constitué en 2009 une équipe d’intervention en cas d’incident relatif à la sécurité informatique, qui travaille en étroite coopération avec la police nationale et qui élabore un cadre national de sécurité cybernétique. Face à ces menaces mondiales, il faut trouver des solutions mondiales, et à ce propos le Pérou est fermement convaincu de l’importance de la coopération internationale et de l’échange d’expériences et de bonnes pratiques, afin de trouver des ripostes efficaces et novatrices. Nous, les États, devons travailler ensemble en utilisant les mécanismes de coordination régionale et internationale.

Dans ce domaine, l’Organisation des Nations Unies joue un rôle essentiel, fondé sur la Stratégie antiterroriste mondiale et sa mise en œuvre globale, coordonnée et équilibrée dans tous ses volets. À cet égard, nous saluons l’action du Groupe de travail sur la protection des infrastructures essentielles de l’Équipe spéciale de lutte contre le terrorisme, et nous l’encourageons à conjuguer les efforts afin de mettre en place les mécanismes nécessaires pour fournir l’assistance technique dont ont besoin les États Membres, lorsqu’ils en font la demande.

De même, ma délégation rappelle l’importance de parachever le processus d’élaboration du projet de convention générale sur le terrorisme international, ainsi que les délibérations sur la question relative à la convocation d’une conférence de haut niveau sous les auspices de l’Organisation des Nations Unies. Dans ce sens, nous lançons un appel pour que l’on redouble d’efforts afin de conduire à ladite convention générale.

Tout en réaffirmant l’attachement du Pérou à la lutte contre les menaces que représentent le terrorisme et l’extrémisme violent, je tiens à vous assurer, Monsieur le Président, que vous pouvez compter sur le soutien constant de ma délégation.

Le Président (*parle en anglais*) : Je donne maintenant la parole à la représentante de la Colombie.

Mme Mejía Vélez (Colombie) (*parle en espagnol*) : Je félicite l’Ukraine de son accession à la présidence du Conseil de sécurité, ainsi que la Directrice de cabinet et les représentants des différentes entités, qui ont partagé avec nous ce matin leurs points de vue sur un sujet de préoccupation au niveau mondial.

Le présent débat a été convoqué à un moment où les attaques terroristes ou la menace de ces attaques restent présentes dans tous les pays du monde, sans aucune distinction. Il est certain que nous affrontons de nouveaux défis qui mettent à l’épreuve nos capacités de prévention et d’élaboration de ripostes efficaces.

S’agissant de la Colombie, la protection des infrastructures essentielles contre les attaques terroristes

a été au cœur de notre programme de gouvernement. Du fait du conflit interne qui, comme cela est bien connu, nous a touchés pendant plus de 50 ans, mon pays a souffert d’actes terroristes dont le but était de déstabiliser le fonctionnement du Gouvernement et de la société. Ces attaques ou tentatives d’attaque visaient des infrastructures pétrolières, des centres de télécommunications, des réseaux électriques, des moyens de transport, des réseaux d’entreposage de gaz et de combustible, des systèmes bancaires et financiers, des systèmes d’approvisionnement en eau et des services d’urgence.

Cela nous a obligés à développer, au sein de nos forces armées, ce que nous appelons les Centres spéciaux de protection des infrastructures essentielles et économiques, ce qui a permis un travail commun entre les communautés, les forces de l’ordre et le secteur privé – à savoir les entreprises qui fournissent ces services –, avec la mise en œuvre d’initiatives telles que l’élaboration de documents sur les normes et de protocoles de sécurité, lesquels sont mis au point conjointement par les organismes de sécurité et les secteurs qui visent à optimiser la sécurité de leurs activités productives. Heureusement, je crois que nous pouvons en parler au passé, car le processus de paix va permettre que ces enseignements et leçons soient partagés avec autrui, et nous espérons que cela sera utile à la communauté internationale.

Conformément à ce qui est souligné dans la note de cadrage du Président (S/2017/104, annexe), mon pays a fait avancer ce travail avec le concours des communautés, en se fondant sur la confiance et le dialogue. Comme l’ont dit ce matin la Directrice de cabinet du Secrétaire général de l’ONU et le Secrétaire général de l’Organisation internationale de police criminelle, les États doivent recenser les vulnérabilités dans tous les secteurs, renforcer la coopération en matière de prévention et d’atténuation et parvenir à une meilleure coopération technique, afin d’augmenter les capacités des États, notamment au moyen d’échanges de renseignements, de bonnes pratiques et d’enseignements tirés.

Selon la Colombie, les actes de terrorisme sont criminels et injustifiables, quels qu’en soient les motifs et les auteurs et où qu’ils soient perpétrés. Le terrorisme ne peut ni ne doit être associé à aucune religion, civilisation, ethnie ou nationalité. Nous réaffirmons notre attachement à prévenir, combattre et éliminer le terrorisme et son financement, conformément aux principes inscrits dans la Charte des Nations Unies, dans le plein respect de la souveraineté des pays, de l’état de droit et du droit international.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de la République islamique d’Iran.

M. Khoshroo (République islamique d’Iran) (*parle en anglais*) : D’entrée de jeu, qu’il me soit permis d’exprimer ma gratitude à la délégation de l’Ukraine pour avoir organisé le présent débat et de remercier les intervenants de leurs contributions.

Je m’associe à la déclaration que fera le représentant de la République bolivarienne du Venezuela au nom du Mouvement des pays non alignés.

Actuellement, nous sommes confrontés à une prolifération d’actes terroristes à un niveau sans précédent. Aucun pays n’est à l’abri de devenir éventuellement victime d’actes terroristes. Les attentats terroristes les plus récents, en particulier ceux commis par Daech et d’autres groupes extrémistes et terroristes, indiquent que les infrastructures essentielles deviennent de plus en plus des cibles de choix pour les opérations terroristes. Les dimensions réelles de cette menace mondiale sont révélées lorsque nous prenons note du fait qu’il y a encore des dizaines de milliers de terroristes, y compris des femmes et des jeunes, provenant de plus de 100 pays et de toutes les régions du monde, qui ont rejoint les rangs d’organisations terroristes. Les actes terroristes contre les infrastructures essentielles sèment la terreur au sein du grand public et ont des conséquences néfastes pour le développement économique et social des États, notamment d’éventuelles perturbations de la prestation des services de base. Il existe donc une nécessité pressante de protéger les infrastructures contre un nombre croissant de diverses attaques terroristes, aussi bien matérielles que visant l’électronique.

Les attaques terroristes contre des infrastructures, telles que l’approvisionnement en énergie et en eau, les institutions financières, les télécommunications, les transports et les structures gouvernementales, peuvent faire des victimes civiles, causer des dommages et des pertes de biens de grande ampleur, perturber le bon fonctionnement des services publics et semer le chaos au sein des sociétés. Elles peuvent également provoquer des dégâts environnementaux considérables et grever lourdement les ressources nationales et les capacités de faire face aux difficultés et aux situations d’urgence.

En conséquence, la protection des infrastructures essentielles doit s’inscrire dans le cadre de la lutte contre le terrorisme et doit être intégrée dans les plans nationaux visant à contrer et à prévenir le terrorisme. Au niveau international, il est également essentiel de renforcer la résilience de la communauté internationale pour ce qui est d’affronter ces menaces, afin de réduire les pertes de vies humaines et de protéger les services essentiels pour nos sociétés.

Les attaques en Turquie, en Iraq, à Bruxelles, en Afghanistan et dans plusieurs pays africains sont les attentats terroristes les plus récents ciblant des infrastructures essentielles. En même temps, nous ne devons pas négliger le fait que le châtiment collectif imposé à des peuples ou les brutalités infligées à des peuples sous occupation étrangère, telles que le blocus qui est exercé depuis des décennies par le régime israélien contre les Palestiniens, constituent également la forme la plus grave du terrorisme, puisque cela prive des générations successives de Palestiniens de leurs infrastructures vitales et de leurs ressources naturelles. Dans les pays où des guerres continuent d’être menées, notamment le Yémen, une grande partie des infrastructures civiles déjà affaiblies a été décimée, ce qui contribue à renforcer l’influence du terrorisme et à déstabiliser la région. Face à la menace mondiale du terrorisme, nous devons renforcer notre volonté politique collective d’affirmer la coopération internationale en matière de lutte contre le terrorisme. Dans le même temps, nous soulignons que toutes les initiatives de lutte contre le terrorisme doivent être menées dans le respect des buts et principes consacrés par la Charte des Nations Unies et le droit international.

Nous devons mettre en place des mécanismes multilatéraux solides si nous voulons contrer la menace mondiale commune du terrorisme. Étant donné qu’il n’existe pas de solutions simples aux phénomènes complexes tels que le terrorisme, seuls de tels mécanismes seront à même de garantir une plus grande cohérence et une meilleure coordination de nos politiques et de prévenir toute manœuvre unilatérale négligente, imprudente ou dangereuse qui serait lancée au nom de la lutte contre le terrorisme.

Pour conclure, nous estimons que l’ONU et les autres organisations internationales et régionales compétentes jouent un rôle central dans la lutte contre le terrorisme et la prévention des conflits. Leur engagement permettra de continuer à renforcer les capacités et d’améliorer l’efficacité des efforts généraux visant à réprimer les actes de terrorisme, notamment ceux qui prennent pour cible les infrastructures essentielles, cela aux niveaux national, régional et international.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de l’Inde.

M. Akbaruddin (Inde) (*parle en anglais*) : Je tiens à vous remercier, Monsieur le Président, d’avoir organisé le présent débat public sur une question qui revêt une importance croissante dans notre monde interconnecté. Nous accueillons par ailleurs avec satisfaction les exposés instructifs et pénétrants qui nous ont été présentés.

De plus en plus, les idées, les secteurs industriels, les marchés, les ressources, les services et les produits que nous partageons sont interconnectés comme jamais auparavant, de la manière dont nous faisons du commerce à la manière dont nous investissons, de la manière dont nous voyageons à la manière dont nous nous alimentons et, de fait, de la manière dont nous pensons à la manière dont nous vivons. Toutes ces activités, d’une manière ou d’une autre, reposent sur la multiplication de réseaux complexes et sensibles. Ces interconnexions, qui sous-tendent l’exercice de fonctions sociétales essentielles, ont suscité une vulnérabilité d’un genre nouveau, donnant aux terroristes la possibilité de menacer des cibles qui dans un autre contexte auraient probablement échappé à leur atteinte. Les menaces de ce type visent à entraîner des perturbations d’une portée qui dépasse largement le voisinage immédiat d’une attaque. Elles ont une incidence beaucoup plus vaste sur la population. Elles forcent les nombreux acteurs qui fournissent des services de base à se tenir constamment sur leurs gardes. Ainsi, non seulement elles accentuent la pression que subissent les parties prenantes et leurs sociétés, mais elles font également augmenter le coût des services fournis.

Les grands centres urbains tels que Mumbai, New York et Londres sont devenus des cibles, car tout coup porté à des villes qui servent de centres financiers peut avoir de multiples répercussions sur l’économie d’un pays. Les enquêtes sur les odieux actes de terrorisme commis à Mumbai en 2008 ont révélé l’influence que voulaient avoir leurs auteurs sur l’âme et l’économie de l’Inde toute entière. Ces attaques, qui ont frappé un hôpital, une gare et des hôtels, ont été soigneusement planifiées et préparées à l’extérieur de nos frontières afin de provoquer une paralysie non seulement dans la vie quotidienne d’une métropole dynamique, mais

également dans la vie d’un pays qui compte un milliard d’habitants.

La protection des infrastructures essentielles relève avant tout de la responsabilité nationale. Cependant, étant donné qu’un grand nombre de nos technologies et des modèles de base sur lesquels sont fondés les systèmes du monde entier sont similaires, la menace d’attaques contre une bourse internationale, un grand barrage, une centrale nucléaire, du sabotage possible d’oléoducs ou de gazoducs ou des systèmes de sécurité aérienne des aéroports, ou du blocage potentiel d’un canal ou d’un détroit international peut avoir des répercussions et entraîner des complications qui dépassent largement les frontières nationales.

Un grand nombre d’attaques terroristes récentes ont montré que l’accès aux technologies de l’information et des communications, et dans certains cas leur manipulation, est un facteur important. La nature mondiale de ces technologies fait ressortir la nécessité d’une vision et d’une coordination internationales sur les aspects de la politique suivie, et ce afin de renforcer nos capacités. Bien qu’ils se préoccupent de cette question depuis des années, les États n’ont adopté qu’un petit nombre d’instruments internationaux portant sur les problèmes résultant des menaces cybernétiques.

Le droit international en vigueur n’est pas adapté pour appuyer des interventions contre les cyberattaques. Les décisions du Conseil de sécurité qui imposent des obligations contraignantes en matière de lutte contre le terrorisme n’en font aucune mention. S’agissant de développer le droit conventionnel, les États Membres négocient un projet de convention générale sur le terrorisme international depuis la seconde moitié des années 90, et cette période correspond à la montée des préoccupations relatives aux cyberattaques terroristes. La définition fournie dans le projet de texte est peut-être assez large pour s’appliquer aux cyberattaques, mais l’éventualité de cyberattaques terroristes ne catalyse toujours pas les négociations même au bout de 20 ans.

Le présent débat nous offre donc la possibilité de nous demander si nous pouvons surmonter nos divergences face aux préoccupations concernant les menaces informatiques qui pèsent sur les infrastructures essentielles, ou s’il faudra attendre un événement cataclysmique pour renforcer la collaboration internationale en matière de protection des infrastructures essentielles contre les cyberattaques terroristes. Étant donné que cette menace est perceptible et qu’elle cause une angoisse compréhensible au niveau mondial, est-il possible d’examiner diverses options en vue de renforcer le droit international pour contrer les cyberattaques terroristes? Le mois dernier, un appui croissant s’est manifesté dans cette salle en faveur d’une approche préventive. Sommes-nous donc prêts à mettre en place une approche collective concertée en matière de répression des cyberattaques terroristes contre les infrastructures essentielles? Si nous ne sommes pas disposés à négocier un traité sur ce type d’attaques, pouvons-nous au moins commencer par clarifier la manière dont les divers traités relatifs à la lutte antiterroriste s’appliquent à ces attaques?

La collaboration est essentielle pour repousser le périmètre de défense du pas de notre porte aux limites de notre voisinage. La protection des infrastructures essentielles contre les cyberattaques terroristes exige de mettre en place un programme de surveillance du voisinage au niveau mondial, car comme le veut l’adage, on se sent plus en sécurité à plusieurs. Toute collaboration efficace repose néanmoins sur la confiance, et la confiance fait actuellement défaut. L’enseignement du passé est que le droit international en matière de terrorisme s’est en grande partie développé du fait de la réaction des États à des actes de violence terroriste. Nous espérons que cette tendance ne se poursuivra pas, et l’adoption aujourd’hui par le Conseil de sécurité de la résolution 2341 (2017) est un premier petit pas dans un domaine où il reste un long chemin à parcourir.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant d’Israël.

M. Roet (Israël) (*parle en anglais*) : Je tiens à féliciter l’Ukraine et le Ministre ukrainien des affaires étrangères de leur accession à la présidence du Conseil de sécurité et à souhaiter plein succès à l’Ukraine au cours du mois. Nous vous remercions, Monsieur le Président, d’avoir convoqué ce débat opportun sur un sujet important, et nous sommes fiers de nous être portés coauteur de la résolution 2341 (2017), adoptée ce matin.

Pour Israël, le présent débat n’est malheureusement pas théorique, car il est confronté à des menaces terroristes depuis sa création. Aujourd’hui, alors que le terrorisme nous menace tous, Israël est situé dans une des régions les plus instables et violentes au monde, et il est menacé de toutes parts. Au nord, nous sommes confrontés au Hezbollah, qui a été désigné internationalement comme un groupe terroriste et dissimule son arsenal de plus de 150 000 roquettes, toutes dirigées vers Israël, dans des habitations civiles, des écoles et des hôpitaux. En menaçant des civils depuis les

rangs de sa propre population, le Hezbollah commet un double crime de guerre, et ses agissements sont pourtant rarement condamnés dans cette salle. En 2016, Hassan Nasrallah, Secrétaire général du Hezbollah, a menacé de lancer, contre les réservoirs d'ammoniaque de la ville d'Haïfa, une attaque de grande ampleur, dont il a affirmé qu'elle ferait des dizaines de milliers de morts et aurait des conséquences pour 800 000 Israéliens. Il a ajouté que cela aurait l'effet d'une bombe nucléaire et qu'il pouvait donc affirmer que le Liban est aujourd'hui doté d'une bombe nucléaire.

Au sud, nous sommes confrontés au Hamas, le groupe terroriste qui contrôle Gaza et appelle ouvertement à la destruction de l'État d'Israël. En outre, le Hamas mène des attaques délibérées contre des civils au sein de sa propre population et prend pour cible des infrastructures essentielles. Nous l'avons constaté en 2014, lorsque le Hamas a essayé de paralyser Israël en attaquant son principal centre de transport international, l'aéroport Ben Gourion.

Comme Israël l'a déjà déclaré dans cette salle, partout où il y a de la terreur, on y retrouve l'Iran également. Par conséquent, la déclaration faite par le représentant de l'Iran il y a quelques minutes m'a fait penser à quelqu'un qui tue ses propres parents et qui demande ensuite grâce au tribunal parce qu'il est orphelin. L'Iran est le principal État qui soutient le terrorisme, qui soutient et appuie les opérations et les activités du Hezbollah, du Hamas et d'autres groupes terroristes basés au Moyen-Orient et ailleurs dans le monde.

L'Iran continue d'effectuer des essais de missiles balistiques de plus en plus perfectionnés, en menaçant directement Israël. La semaine dernière, le 4 février, un haut responsable de la Commission de la sécurité nationale et de la politique étrangère du Parlement iranien a déclaré qu'« il faut seulement sept minutes pour que le missile iranien frappe Tel-Aviv ». Le tir d'essai de ce missile balistique prouve encore une fois que l'Iran fait fi de la résolution 2231 (2015). J'appelle le Conseil de sécurité à réagir fermement et énergiquement à ces violations et provocations de la part de l'Iran.

Nous avons été récemment témoins d'une vague d'attaques terroristes contre des infrastructures essentielles dans le monde entier, notamment par Daech. L'avion de la compagnie EgyptAir abattu au-dessus de la Méditerranée, l'attentat perpétré à l'aéroport Atatürk à Istanbul et les attentats qui ont visé la station de métro et l'aéroport de Bruxelles ont fait des centaines de morts et de blessés, prouvant une fois de plus qu'aucun pays n'est en sécurité et que personne n'est à l'abri de ces attaques ignobles.

Du transport mondial aux systèmes financiers, en passant par les infrastructures énergétiques aux services d'approvisionnement en eau, les attaques contre les infrastructures essentielles menacent les fondements mêmes sur lesquels repose notre société moderne. Les terroristes sont conscients que les attaques contre des infrastructures essentielles peuvent faire des ravages qui vont bien au-delà de la cible visée. Les attaques contre les grands réseaux d'infrastructures peuvent paralyser des pays et des régions entiers.

Chaque jour, nous devons nous adapter aux menaces terroristes en évolution constante contre nos infrastructures, nos civils et nos citoyens. Nous sommes conscients que le seul moyen de contrer ces menaces est de prendre les devants, de rester vigilants et d'anticiper les actes des auteurs de ces crimes. Les réalités d'aujourd'hui n'exigent pas seulement que nous luttions face aux attaques physiques. Nous nous battons désormais sur un front tout nouveau, car nous devons également nous protéger contre les cybermenaces et les cyberattaques.

Les infrastructures essentielles sont étroitement liées à la technologie et aux dangers y relatifs, à savoir les cyberattaques. Les cyberattaques n'ont pas de frontières et ne sont pas uniquement le fait des acteurs étatiques. Ceux qui mènent de telles attaques ne sont pas limités par des barrières physiques et peuvent causer des dommages bien plus graves qu'un attentat terroriste physique qui ne vise qu'un endroit bien précis. Grâce à sa culture en matière de sécurité à la pointe du progrès technique et aux cyber-entreprises communes des secteurs privé et public, Israël a réussi à contrer des menaces qui pesaient sur des systèmes privés et publics.

On dit que la nécessité est mère de l'invention. Par nécessité, nous sommes devenus des experts en matière de lutte contre le terrorisme et c'est avec fierté que nous partageons nos connaissances avec les gouvernements du monde entier. Les experts israéliens appliquent leurs compétences spécialisées à un large éventail de questions – du financement du terrorisme aux enquêtes scientifiques en passant par la sécurité de l'aviation et la protection des frontières. Ces activités reflètent notre conviction fondamentale qu'une lutte efficace contre le terrorisme passe par la coopération internationale. Une menace internationale grave appelle une riposte internationale sérieuse. Nous sommes

déterminés à prendre toutes les mesures qui s'imposent pour continuer de protéger nos citoyens et de partager nos connaissances avec la communauté internationale.

Le Président (*parle en anglais*) : Je donne maintenant la parole à S. E. M. Vale de Almeida, Chef de la délégation de l'Union européenne auprès de l'Organisation des Nations Unies.

M. Vale de Almeida (Union européenne) (*parle en anglais*) : J'ai l'honneur de prendre la parole au nom de l'Union européenne de ses 28 États membres.

L'ex-République yougoslave de Macédoine, le Monténégro, la Serbie et l'Albanie, pays candidats; la Bosnie-Herzégovine, pays du Processus de stabilisation et d'association et candidat potentiel; ainsi que l'Ukraine et la République de Moldova s'associent à la présente déclaration.

Tout d'abord, je voudrais féliciter l'Ukraine qui assure actuellement la présidence du Conseil de sécurité et remercier la Suède de son excellente présidence du mois dernier. Je tiens à féliciter l'Ukraine d'avoir organisé le débat d'aujourd'hui, qui nous donne une occasion de parler de la protection des infrastructures essentielles, une source de vive préoccupation pour l'Union européenne et ses États membres. Je voudrais également souligner que nous devons œuvrer de concert en la matière au niveau international pour garantir un degré élevé de protection à nos infrastructures essentielles et pour renforcer leur résilience face aux attentats terroristes et autres perturbations.

Les questions soulevées dans la note de cadrage (S/ 2017/104, annexe) sont très importantes. J'aimerais les aborder brièvement, l'une après l'autre.

S'agissant de la première question concernant les instruments, en Europe, nous avons mis en place le Programme européen de protection des infrastructures critiques. En place depuis 2006, ce programme définit le cadre général des activités visant à améliorer la protection des infrastructures critiques dans l'Union européenne dans tous les secteurs d'activité économique concernés. Ce programme vise à faire face non seulement aux menaces terroristes, mais également aux menaces d'origine humaine et technologique et aux catastrophes naturelles. En bref, il propose une stratégie qui couvre tous les secteurs et tous les risques. Ce programme repose sur des échanges réguliers d'informations entre les États membres de l'Union européenne dans le cadre des réunions des points de contact pour la protection des infrastructures critiques.

L'un des piliers du programme est la directive européenne de 2008 sur la protection des infrastructures critiques, qui établit une procédure pour le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection. Il s'agit d'infrastructures essentielles situées dans des États membres dont la perturbation ou la destruction aurait des effets importants sur au moins deux États membres. Cette directive a une portée sectorielle et s'applique aux secteurs de l'énergie et des transports.

La directive exige en outre des propriétaires et des opérateurs d'infrastructures critiques européennes désignées d'élaborer des plans de sécurité des opérateurs – plans de continuité des activités avancés – et de désigner des correspondants pour la sécurité pour faciliter la communication entre le propriétaire ou l'opérateur et les autorités nationales compétentes en matière de protection des infrastructures critiques. L'application de la directive est contrôlée par des points de contact désignés par chaque État membre de l'Union européenne. Le groupe des points de contact travaille également en coordination avec la Commission européenne en ce qui concerne la coopération internationale en dehors de l'Union européenne – jusqu'ici avec les États-Unis et le Canada –. Toutefois, cette année, nous commencerons également à coopérer avec les pays voisins en Europe de l'Est et dans les Balkans.

Pour faire face aux nouvelles menaces, en 2016, l'Union européenne a adopté le Cadre commun en matière de lutte contre les menaces hybrides, qui couvre également la question de la protection des infrastructures critiques contre les menaces hybrides et asymétriques, notamment dans les secteurs de l'énergie et des transports. Ce cadre vise à renforcer la résilience des États membres dans ce domaine et prévoit une coopération avec les partenaires de l'Union européenne pour lutter contre ces menaces.

S'agissant de la deuxième question relative aux méthodes que les États doivent privilégier pour favoriser la réactivité et la résilience face aux attaques terroristes ciblant des infrastructures essentielles, la Commission européenne a financé plus de 120 projets dans le cadre d'un programme spécifique pour la période 2007-2013 visant à soutenir les projets en matière de prévention, préparation et gestion des conséquences des attaques terroristes et autres risques liés à la sécurité. Ce programme vise à protéger les citoyens

et les infrastructures critiques des attaques terroristes et d’autres incidents de sécurité en promouvant la prévention et la préparation, en renforçant la protection de ces infrastructures et en améliorant la gestion des crises. Un objectif important à cet égard est de mettre à disposition les connaissances spécialisées et les données scientifiques nécessaires pour mieux comprendre les criticités et les interdépendances. En outre, suite à l’augmentation des cyber-menaces, l’Union européenne a adopté une législation sur la sécurité des réseaux et des systèmes d’information en juillet 2016.

Pour ce qui est de la troisième question, qui porte sur la façon de renforcer les capacités des secteurs public et privé en vue de prévenir aux attaques et de réagir aux menaces pesant sur les infrastructures essentielles, les programmes de formation et les exercices se sont avérés être des outils très utiles, que l’Union européenne a promus et utilisés. Un bon exemple en est l’exercice VITEX 2016, qui a été conçu et coordonné par la présidence néerlandaise de l’Union européenne. Ce fut le premier exercice à l’échelle de l’UE portant sur les incidences d’une défaillance à large échelle d’une infrastructure essentielle – dans ce cas électrique – sur toute l’Europe. L’exercice VITEX 2016 a donné à l’élaboration d’un guide décrivant étape par étape comment un tel exercice peut être organisé. Ce guide est mis à la disposition de tout un chacun afin d’encourager d’éventuels exercices de suivi à l’avenir.

S’agissant du quatrième point, à savoir les mécanismes et les plateformes de coopération, je voudrais souligner l’importance fondamentale de l’échange régulier d’informations et de pratiques optimales. La Commission européenne a mis en place à cet effet le Réseau d’alerte concernant les infrastructures critiques, un système multidimensionnel permettant aux États Membres et aux parties prenantes clefs d’échanger, sur Internet, les idées, les études et les pratiques optimales sur la protection des infrastructures essentielles. Ce portail qui est opérationnel depuis la mi-janvier 2013 vise aussi à mieux sensibiliser et à contribuer à la protection des infrastructures critiques en Europe.

Pour ce qui est de mon dernier point, à savoir le rôle de l’ONU et de ses institutions dans ce travail, il est certainement possible de renforcer la coopération vu que la sécurité et la protection des infrastructures critiques est un motif de préoccupation pour nous tous, comme l’est la lutte contre le terrorisme. L’Union européenne aimerait coopérer à l’échelle internationale avec des partenaires au-delà de ses frontières en matière de protection des infrastructures critiques contre cette menace commune. Nous sommes déjà engagés dans divers forums, comme l’Organisation pour la sécurité et la coopération en Europe et le Conseil de l’Europe, mais nous saluons les initiatives prises par les Nations Unies dans ce domaine, et nous sommes disposés à étudier les possibilités d’une telle coopération.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de la Roumanie.

M. Jinga (Roumanie) : Je tiens à remercier la présidence ukrainienne du Conseil de sécurité pour l’initiative d’inscrire pour la première fois à l’ordre du jour du Conseil le thème consacré à la protection des infrastructures critiques contre les attaques terroristes. Je voudrais remercier également les invités qui, par leurs interventions, ont enrichi le présent débat public.

La Roumanie souscrit pleinement à la déclaration de l’Union européenne. J’ajoute maintenant quelques observations à titre national.

Les infrastructures de transport, les télécommunications, les réseaux de distribution d’énergie ou d’eau, les systèmes financiers ou les services d’urgence – ce que l’on appelle infrastructures critiques – sont essentielles au bon fonctionnement de notre société contemporaine. Par conséquent, leur protection constitue une grande priorité. Les entités terroristes ont montré qu’elles possédaient la capacité d’agir avec ténacité, rapidité et souplesse. Vu leur objectif de causer le plus grand nombre de victimes et de dégâts, les infrastructures critiques restent une cible préférée. La dimension mondiale des menaces et des attaques de nature terroriste exige une réponse mondiale et les Nations Unies doivent jouer un rôle clef en vue d’une approche coordonnée et efficace. Étant donné les connexions interétatiques des infrastructures critiques, la coopération régionale et internationale est aussi fondamentale. Au cours des dernières années, les actes terroristes visant les infrastructures critiques ont mis en exergue la vulnérabilité des États. Nous avons tous en mémoire les plus récents cas qui ont démontré l’incidence des attaques terroristes perpétrées contre les aéroports de Bruxelles et d’Istanbul. Il ne faut pas oublier les attaques les plus meurtrières dans l’histoire de l’Espagne contre les trains de voyageurs à Madrid, en 2004.

De plus, la communauté internationale a été témoin des horreurs commises contre les civils en Syrie, où l’eau est devenue une arme de guerre, lorsque plus

de 5 millions d'habitants de la capitale ont été privés d'eau pendant plus d'un mois après l'attaque contre la principale source d'approvisionnement en eau. On note aussi la destruction en 2013 du pont suspendu de Deir el-Zor, sur l'Euphrate, coupant l'accès à cette ville d'environ 50 000 âmes, ou les attaques perpétrées par Daech qui ont visé les puits de pétrole, les raffineries et les centrales électriques en Syrie et en Iraq. Malheureusement, la liste n'est pas exhaustive. Aucun État n'est entièrement à l'abri de telles attaques.

La Roumanie a élaboré en 2011 une stratégie nationale portant sur la protection des infrastructures critiques, et nous sommes d'avis que dans le cadre des démarches destinées à protéger les infrastructures critiques, il faut placer davantage l'accent sur la coopération entre les autorités étatiques, les opérateurs économiques et la population, ainsi que sur l'analyse des risques et sur l'interopérationnalisation du partenariat public-privé. Ce dernier est essentiel, vu qu'une partie significative des infrastructures appartient aux compagnies privées ou multinationales.

Parmi les moyens exploités par les entités terroristes et qui offrent d'immenses possibilités, il y a les technologies de l'information et des communications en ligne, qui ont connu une dynamique sans précédent. L'expérience a montré que les plus graves menaces terroristes sont de nature mixte, ce qui permet que les attaques cybernétiques aient une incidence directe sur les infrastructures physiques. Dans ce contexte, l'importance de la prévention devient encore plus significative.

La Roumanie a adopté en 2013 une Stratégie de sécurité cybernétique et un Plan d'action national pour sa mise en œuvre. De plus, mon pays a mis en place en 2011 le Centre national de réponse aux incidents de sécurité cybernétique, chargé de fournir des services publics de prévention, de réaction et de conseil. Actuellement, le Centre met en œuvre un projet où nous sommes partenaires avec 27 organisations provenant de 14 pays européens.

Un autre moyen efficace pour lutter contre 1e terrorisme est la prévention de l'extrémisme violent, un domaine où la Roumanie a également beaucoup investi, avec des résultats qui parlent d'eux-mêmes. Mon pays n'est pas confronté au phénomène des combattants terroristes étrangers, et nous n'avons enregistré aucun cas de citoyens roumains ou de ressortissants étrangers voyageant vers les théâtres de guerre en vue de s'affilier aux entités terroristes. De surcroît, en Roumanie la propagande du djihad n'existe que d'une manière extrêmement isolée.

Nous apprécions hautement les efforts de l'ONU visant à développer un cadre juridique et institutionnel de lutte contre les menaces terroristes, en tant qu'instrument mis à la disposition des États Membres. La Roumanie a coparrainé la résolution 2341 (2017) sur la protection des infrastructures essentielles contre les attaques terroristes, adoptée aujourd'hui à l'unanimité par le Conseil de sécurité. Celle-ci s'ajoute à l'adoption, en 2016, de la résolution 2322 (2016) sur la coopération judiciaire internationale, de la résolution 2309 (2016) concernant la lutte contre les menaces contre l'aviation civile, et de la résolution 2286 (2016) portant sur la protection du personnel médical et des installations médicales en temps de conflit armé. Un autre pilier important demeure l'adoption par l'Assemblée générale de la résolution 71/19 sur la coopération entre l'Organisation des Nations Unies et l'Organisation internationale de police criminelle (INTERPOL).

Enfin, nous saluons la décision du Secrétaire général de lancer un débat approfondi sur la mise en œuvre de la Stratégie antiterroriste mondiale des Nations Unies. La discussion informelle qui sera organisée par l'Assemblée générale représente ainsi un bon point de départ pour renforcer la composante antiterroriste au niveau des Nations Unies.

Pour terminer, la Roumanie considère que, dans le cadre des efforts visant à assurer la protection des infrastructures critiques contre les attaques terroristes, le respect du cadre juridique international et l'adoption et l'application des lois nationales sont essentiels.

Le Président : Je donne maintenant la parole au représentant de la Belgique.

M. Buffin (Belgique) : Nous remercions la présidence ukrainienne du Conseil de sécurité d'avoir programmé le présent débat public sur le thème important de la protection des infrastructures critiques contre la menace terroriste. Nous remercions également les différents intervenants invités au présent débat de leurs interventions.

La Belgique souscrit pleinement à la déclaration de l'Union européenne.

Face au terrorisme et à l'extrémisme violent, des réponses multiples s'imposent. Il importe d'abord de s'attaquer aux causes profondes du phénomène en défendant collectivement les valeurs fondamentales

que sont le respect des droits de l'homme et de l'état de droit, la bonne gouvernance, le développement durable, la lutte contre l'impunité et la promotion de la tolérance. Il importe également que la communauté internationale unisse ses efforts pour favoriser le règlement pacifique et politique des trop nombreux conflits qui secouent 1a planète.

La Syrie offre l'exemple dramatique le plus évident. Mais ce n'est malheureusement pas le seul foyer de conflit. D'autres régions du monde connaissent en effet la guerre et une instabilité propice au développement de l'influence des groupes terroristes. Et à cet égard, nous souhaiterons souligner la responsabilité particulière qui incombe au Conseil de sécurité d'unir la communauté internationale aux fins du règlement pacifique et politique de ces conflits. Et puis, bien entendu, il est nécessaire de lutter directement contre Daech, Al-Qaida et ceux qui s'en réclament. La Belgique s'implique activement, à cet égard, dans la coalition internationale contre Daech.

S'agissant plus particulièrement de la protection des infrastructures critiques, je souhaiterais faire les commentaires suivants. Dans ce domaine, comme dans d'autres, l'importance de la prévention est capitale. À cet égard, il convient de développer des méthodes modernes de prévention reposant sur la formation adéquate des agents de sécurité et des forces de l'ordre. La Belgique accorde une grande importance à ces aspects, notamment via l'organisation d'exercices et la mise en place de programmes de formation spécifique pour ses forces de l'ordre.

Le plan de sécurité des infrastructures critiques doit contenir aussi bien des mesures physiques, comme le placement de barrières de sécurité ou de caméras de surveillance, que des mesures cyber telles que les pare-feux ou systèmes de détection. Les autorités doivent, par ailleurs, veiller à développer les outils numériques de planification d'urgence, de gestion des crises et d'alerte des populations directement concernées par une situation d'urgence. En Belgique, par exemple, le Centre pour la Cybersécurité Belgique, créé en 2014, a élaboré un plan national qui décrit les rôles et les tâches des différentes autorités en cas d'incident national ou de crise nationale de cybersécurité.

Une coopération efficace entre secteurs public et privé constitue un autre axe important en termes de prévention et de réaction à la menace, car il n'est pas rare que les infrastructures critiques appartiennent au secteur privé. Il convient donc de multiplier les occasions pour les secteurs public et privé de se rencontrer notamment par le biais de conférences, d'exercices ou de formations. L'établissement d'un réseau d'information entre entreprises privées et autorités publiques contre les menaces terroristes constitue, à cet égard, un outil fort important.

Le renforcement de la coopération internationale, notamment par le biais d'échange d'informations, de la tenue d'exercices conjoints et de l'élaboration de scénarii et de plans d'urgence, doit absolument être encouragé. Dans cette perspective, l'Union européenne a élaboré, avec ses États membres, divers outils en vue de faire face à la menace, notamment le Programme européen de protection des infrastructures critiques et la directive européenne du 6 juillet 2016 relative à la sécurité des réseaux et des systèmes d'information au sein de l'Union européenne. Ces outils, ainsi que d'autres, ont été détaillés dans son intervention par le représentant de l'Union européenne. Je n'y reviendrai donc pas.

S'agissant de l'ONU, il convient de souligner le rôle important qu'elle a à jouer, notamment par le biais du Comité contre le terrorisme, de la Direction exécutive qui assiste le Comité, et de l'Équipe spéciale de lutte contre le terrorisme. Ces organes peuvent utilement œuvrer à sensibiliser davantage les États Membres au thème de la protection des infrastructures critiques contre les menaces terroristes en favorisant les échanges de bonnes pratiques dans le cadre opérationnel. Cette sensibilisation pourra inclure, par exemple, l'organisation de rencontres où les États partageront les leçons de leur propre expérience et exposeront les pratiques optimales qui ont fait leurs preuves. L'ONU constitue un forum important pour développer l'échange d'informations et de bonnes pratiques et aider à l'identification de lacunes en matière de protection des infrastructures critiques. C'est pourquoi la Belgique a coparrainé la résolution 2341 (2017) adoptée en début de séance.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de l'Argentine.

M. Garcia Moritán (Argentine) (*parle en espagnol*) : Je voudrais tout d'abord remercier la présidence ukrainienne de l'invitation à participer au présent débat public sur une question aussi importante pour la communauté internationale.

L'Argentine condamne le terrorisme sous toutes ses formes et manifestations, et estime que les actes de terrorisme constituent une menace non seulement à la paix et à la sécurité internationales, mais aussi à la

dignité humaine, à la coexistence pacifique et civilisée, à la stabilité et à la consolidation de la démocratie, et au développement socioéconomique des pays. Notre pays, qui a été victime d’attentats terroristes sanglants dans les années 90, réaffirme que les actes de terrorisme sont criminels et injustifiables, quelles qu’en soient les motivations, quel que soit le lieu où ils sont commis et quels qu’en soient les auteurs.

L’on ne peut combattre le terrorisme uniquement en appliquant des mesures de défense ou de sécurité. Il faut, au contraire, adopter une approche globale, telle que reflétée dans la Stratégie antiterroriste mondiale des Nations Unies, sur la base d’une mise en œuvre équilibrée de ses quatre piliers et dans le strict respect du droit international, du droit international des droits de l’homme, du droit international humanitaire et du droit international des réfugiés.

Les infrastructures essentielles sont celles qui sont indispensables au bon fonctionnement des services fondamentaux de la société – la santé, la sécurité, la défense, le bien-être socioéconomique des citoyens et le fonctionnement efficace de l’État – et dont la destruction ou la perturbation totale ou partielle compromet ces services ou les limite considérablement. C’est pourquoi nous nous félicitons de l’approche choisie pour ce débat, vu l’urgence de la menace que représente le terrorisme pour les infrastructures et services essentiels de nos pays. En ce sens, il est nécessaire de renforcer la coopération, la coordination et l’échange d’informations entre les institutions et les organisations de chaque pays, ainsi qu’entre les différents pays. Il faut également s’adapter à la nature changeante de la menace terroriste, tant physique que cybernétique.

Nous nous félicitons de la résolution 2341 (2017) que le Conseil vient d’adopter ce matin et qui est la première à se concentrer spécifiquement sur la question de la protection des infrastructures essentielles. Nous sommes d’accord pour dire qu’il faut exhorter les États à élaborer et à améliorer leurs stratégies d’évaluation et de réduction des risques et à coopérer dans ce sens. La collaboration entre les secteurs public et privé dans ce domaine est également essentielle pour atténuer les risques et prévenir les attaques contre ce type d’infrastructures.

Conscientes de l’importance de s’attaquer sans délai à ce problème, nos autorités ont créé un groupe de travail au sein du Ministère de la modernisation afin d’élaborer les grandes lignes d’un plan d’action visant à identifier et à élaborer des normes et des mesures de protection des infrastructures essentielles, notamment celles de l’information. Le groupe de travail est chargé de définir les critères permettant d’identifier les infrastructures, les secteurs concernés, les organes de réglementation et les entreprises ou organisations responsables. Il doit également élaborer une méthode de travail permettant d’évaluer les risques et d’appliquer des mesures pour les gérer, selon une approche interinstitutionnelle faisant intervenir tous les secteurs concernés.

S’agissant de la cybersécurité, nous estimons qu’il est impératif de respecter des niveaux adéquats de sécurité dans l’univers numérique afin que les technologies de l’information et des communications (TIC) puissent réaliser pleinement leur potentiel. Cela exige un engagement fort de la part de la communauté internationale pour éviter et réprimer l’utilisation abusive des outils technologiques par différents acteurs étatiques et non étatiques. Il faut, toutefois, rappeler que les acteurs non étatiques qui s’en prennent à la sécurité du réseau en utilisant les TIC sont très divers, qu’il s’agisse de groupes terroristes, d’organisations criminelles transnationales ou de délinquants agissant seuls. Pour faire face à ces menaces, il est nécessaire de disposer d’instruments juridiques internationaux spécifiques et distincts grâce auxquels l’on peut mettre en place des systèmes efficaces de coopération internationale pour la prévention, la poursuite et la répression de ces comportements.

Enfin, nous réaffirmons le rôle central que joue l’ONU dans la lutte contre le terrorisme, en tant que pilier du système multilatéral et organisation à composition universelle, dont la responsabilité principale est le maintien de la paix et de la sécurité internationales. Nous sommes convaincus que l’action multilatérale menée à travers l’ONU, conformément aux principes de l’Organisation, nous permettra d’affronter la menace du terrorisme dans le plein respect du droit international des droits de l’homme et du droit international humanitaire, et d’instaurer ainsi un monde plus sûr pour tous.

Le Président (*parle en anglais*) : Je donne maintenant la parole à l’Observateur permanent de l’État observateur du Saint-Siège auprès de l’Organisation des Nations Unies.

Mgr Auza (Saint-Siège) (*parle en anglais*) : La suite sans fin d’attaques terroristes qui frappent les villes et les villages continue de nous rappeler la menace qu’elles représentent pour les infrastructures civiles et les populations civiles. Cette vague de terreur, qui

considère les civils innocents comme les cibles légitimes d’une violence directe ou indirecte qui détruit les infrastructures dont ils dépendent, doit être repoussée par l’action d’une communauté internationale unie.

Les récents conflits dans la région de l’ancienne Mésopotamie ont eu un effet dévastateur sur des minorités ethniques, religieuses et culturelles séculaires qui sont installées dans cette zone depuis des millénaires. Les parties à ces conflits ont cherché à anéantir délibérément le tissu culturel et les racines historiques de ces communautés en détruisant leurs sites religieux et leur patrimoine culturel. La destruction intentionnelle des infrastructures essentielles pour la survie de ces communautés, tels les écoles, les hôpitaux, les réseaux d’approvisionnement en eau et les lieux de culte, est devenue une stratégie pour les anéantir totalement, un moyen de les appauvrir et de les éliminer en s’en prenant aux structures qui leur permettent un minimum de vie communautaire.

Conformément à la Charte des Nations Unies, la communauté internationale a l’obligation de protéger les civils et leurs infrastructures essentielles de la violence et de la barbarie des groupes terroristes. Cette obligation impose notamment de faire davantage connaître cette tactique terroriste et d’exhorter les États à maintenir un haut niveau de protection et de résilience pour les infrastructures essentielles, mais aussi à préparer du mieux possible la population en cas d’attaque et à faire en sorte que les services essentiels ne soient pas interrompus et qu’aucune vie humaine ne soit perdue. Ma délégation estime que le présent débat répond à ce besoin.

Les mesures durables pour renforcer plus efficacement la protection des infrastructures essentielles contre les attaques terroristes doivent se fonder sur des politiques qui rejettent la recherche effrénée du profit et les intérêts géopolitiques étroits même s’ils sont synonymes de destruction des infrastructures civiles essentielles. À cet égard, ma délégation souhaite réitérer l’appel du Saint-Siège aux pays qui produisent des armes afin de sévèrement limiter et contrôler la production et la vente de ces armes, de leurs munitions et des technologies connexes aux pays et aux régions instables où il est très probable qu’elles seront utilisées illégalement et tomberont entre les mains d’acteurs non étatiques.

La communauté internationale doit également s’attaquer au rôle de la criminalité organisée dans la vente et le troc d’armes capables de détruire des infrastructures essentielles. Il faut encourager vigoureusement les États à collaborer dans ce domaine, aux niveaux international et régional, en partageant les informations et les meilleures pratiques, en coordonnant les politiques et en contrôlant de manière conjointe les frontières.

Le monde doit agir pour empêcher les terroristes d’avoir accès à l’appui financier fourni par ceux qui soutiennent le terrorisme. Le caractère sans frontières des groupes terroristes qui détruisent des infrastructures essentielles nécessite que la communauté internationale contrôle les cybertechnologies dont se servent les groupes violents pour recruter de nouveaux adhérents, financer leurs activités et coordonner des attaques terroristes.

Le pape François a à plusieurs reprises décrit notre époque comme une époque de guerre, celle de la troisième guerre mondiale menée par morceaux et dans laquelle nous sommes témoins tous les jours de crimes sauvages, de massacres atroces et de destructions insensées, comme celle des infrastructures essentielles à l’existence de populations entières.

La communauté internationale doit s’unir pour mettre fin à cette guerre menée par morceaux. Cette unité est indispensable si la communauté internationale veut atteindre cet objectif commun qu’est la protection des infrastructures essentielles contre les attaques terroristes. Cet objectif nous l’atteindrons plus rapidement et plus efficacement si les États partagent sans égoïsme les informations critiques, les meilleures pratiques et les ressources technologiques, en particulier avec ceux qui sont le moins en mesure de protéger leurs infrastructures essentielles et leurs populations contre les attaques terroristes.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de la Turquie.

M. Begeç (Turquie) (*parle en anglais*) : Tout d’abord, je tiens à remercier l’Ukraine d’avoir organisé ce débat public, qui fait suite à la réunion très utile qu’elle avait convoquée selon la formule Arria en novembre dernier. Je veux aussi remercier les intervenants de leurs exposés. La Turquie se félicite de l’adoption de la résolution 2341 (2017), dont elle est l’un des coauteurs.

À l’avant-poste de la lutte contre le terrorisme, la Turquie combat en ce moment-même et de façon simultanée plusieurs organisations terroristes. Nous ne savons que trop les souffrances profondes, les dommages et les pertes en vies humaines qui sont infligées à des

individus, des familles et des sociétés tout entières. Ces 18 derniers mois, plus de 500 innocents ont perdu la vie et bien davantage encore ont été blessés en Turquie dans des attentats terroristes perpétrés par Daech et le Parti des travailleurs du Kurdistan (PKK).

Les organisations terroristes sont parfaitement conscientes des dommages que leurs attaques peuvent causer aux infrastructures essentielles. En plus des pertes matérielles et humaines, les attaques contre les infrastructures essentielles, notamment dans les secteurs de l'énergie, des transports, des télécommunications, de la défense ou de l'industrie chimique, peuvent potentiellement perturber l'ordre public et la prestation de services publics essentiels, mettant ainsi en péril le bon fonctionnement et la prospérité de la société, comme le souligne la note de cadrage élaborée par le Président (voir S/2017/104, annexe).

La Turquie est la cible de telles attaques. En juin 2016, Daech s'en est pris à l'aéroport Atatürk d'Istanbul, tandis que le PKK a visé pour sa part des barrages hydrauliques, des pipelines, des installations de santé et des institutions publiques et privées, y compris des écoles, des établissements éducatifs et des infrastructures médicales. Le PKK a également enlevé des fonctionnaires, notamment des membres des services sanitaires, éducatifs et des douanes. En outre, des institutions de l'État, dont le Parlement turc, ont été bombardées par l'organisation terroriste de Fethullah Gülen durant le coup d'État manqué du 15 juillet 2016.

Face aux graves menaces posées par de multiples organisations terroristes, la Turquie a pris un certain nombre de mesures pour protéger la vie de sa population, ainsi que les institutions et investissements publics et privés. La Turquie accorde une importance particulière à la sécurité de ses infrastructures énergétiques essentielles, en raison de la demande croissante en énergique portée par une croissance économique nationale toujours plus forte mais aussi du fait de sa position géostratégique, qui en fait une voie d'approvisionnement durable entre régions productrices et régions consommatrices. Une des mesures que nous avons prises qui s'est avérée particulièrement utile a été la mise en place de comités pour la sécurité des infrastructures énergétiques essentielles et des pipelines, placés sous l'autorité du Ministère de l'énergie et des ressources naturelles.

Protéger les infrastructures essentielles contre les attaques terroristes est un défi complexe qui requiert la participation du secteur public et du secteur privé ainsi que la protection des infrastructures transfrontières et une préparation au niveau international. La coopération internationale et la mise en commun des meilleurs pratiques sont donc indispensables. C'est pourquoi de nombreuses organisations internationales et régionales, dont l'OTAN, l'Organisation pour la sécurité et la coopération en Europe et l'Union européenne, se penchent tout particulièrement sur cette question.

En tant que pays qui est attaché à la centralité du travail de l'ONU dans les efforts mondiaux pour lutter contre le terrorisme, nous rappelons que la protection des infrastructures essentielles est aussi l'un des objectifs inclus dans la Stratégie antiterroriste mondiale des Nations Unies, adoptée en 2006. Nous remercions la Directrice de cabinet de l'aperçu qu'elle a donné du travail entrepris par l'ONU sur cette question. Nous espérons que l'Organisation va poursuivre ses efforts en ce sens, en coordination étroite avec d'autres organisations internationales et régionales confrontées elles aussi à ce problème.

À cet égard, je voudrais évoquer également l'importance de protéger les cibles vulnérables, notamment les centres religieux, les sites touristiques et les transports publics terrestres, ainsi que les installations commerciales telles que les hôtels, les restaurants, les stades et les salles de spectacle, où les gens se réunissent et qui sont relativement vulnérables aux attaques terroristes du fait de leur libre accès et de leur sécurité limitée. Les préoccupations en matière de protection des cibles vulnérables ne sont pas nouvelles. Mais les groupes terroristes s'en prennent de plus en plus à ces sites, comme nous l'avons vu lors des attaques terroristes perpétrées à Istanbul près d'un stade de football en décembre 2016 etu dans une discothèque, le 1er janvier 2017, dans lesquelles de nombreux Turcs ainsi que des ressortissants étrangers ont trouvé la mort.

C'est dans ce contexte que la réunion inaugurale sur la « Protection des cibles vulnérables dans le contexte d'une initiative antiterroriste », codirigée par l'ONU et la Turquie sous les auspices du Forum mondial de lutte contre le terrorisme, s'est tenue à Antalya, en Turquie, en décembre 2016. Nous espérons que le répertoire des bonnes pratiques pour améliorer la sécurité et la résilience des sites qui sont des cibles vulnérables potentielles, qui doit être établi dans le cadre de cette initiative à l'issue d'une série d'ateliers régionaux qui auront lieu en 2017, pourra servir de point de départ à une coopération, une assistance et une

formation internationales en vue de renforcer la sécurité et la résilience des cibles non protégées.

Comme je l'ai dit avec insistance, la protection des infrastructures essentielles contre les attaques terroristes est un défi que nous devons relever ensemble. La coopération internationale est vitale. Nous appuyons le travail réalisé dans ce domaine par les organisations internationales et régionales. Nous estimons que l'ONU et ses organismes ont un rôle particulier à jouer à cet égard, et nous sommes prêts à soutenir toutes les initiatives qui pourraient être menées à cette fin.

Le Président (*parle en anglais*) : Je donne maintenant la parole à la représentante de Cuba.

Mme Rodríguez Camejo (Cuba) (*parle en espagnol*) : Cuba souscrit sans réserve à la déclaration que fera le représentant du Venezuela au nom du Mouvement des pays non alignés.

Notre pays réitère sa volonté inébranlable de lutter contre le terrorisme et exprime son rejet et sa condamnation énergiques de tous les actes, méthodes et pratiques terroristes, sous toutes leurs formes et dans toutes leurs manifestations, quelles qu'en soient les motivations, y compris le terrorisme d'État.

Cuba, conformément aux 18 conventions internationales relatives au terrorisme auxquelles elle est partie, a mis en place des mesures juridiques pertinentes, telles que la loi 93 sur les actes de terrorisme. Le peuple cubain a subi dans sa propre chair les conséquences d'actes terroristes organisés, financés et exécutés depuis l'étranger, lesquelles se sont traduites par un bilan de 3 478 morts et 2 099 handicapés. Le Gouvernement cubain n'a jamais permis ni ne permettra jamais l'utilisation de son territoire national pour mener, planifier, appuyer, dissimuler ou financer des actes de terrorisme prenant pour cible un autre État, sans exception aucune. Notre pays est favorable à l'adoption d'une convention générale sur le terrorisme, ainsi qu'à la convocation, sous les auspices de l'Organisation des Nations Unies, d'une conférence internationale qui nous permettrait de parvenir à une réponse multilatérale au terrorisme. Nous rejetons et condamnons la politique de deux poids deux mesures et la sélectivité dans le traitement de cette question. La lutte contre le terrorisme ne peut servir de prétexte à l'ingérence, à l'interventionnisme, à l'agression ou aux violations du droit international et du droit des droits de l'homme. Nous demandons que les groupes terroristes cessent d'être financés, équipés et formés, et qu'ils ne reçoivent plus ni armes ni quelque forme de soutien que ce soit.

À la lumière de la militarisation du cyberespace et de la prolifération de la cybercriminalité et du cyberterrorisme, il est de plus en plus urgent que les États veillent à ce que les technologies de l'information et des communications, Internet, la télévision, la radio et d'autres parties de leurs infrastructures essentielles ne soient pas utilisés par des groupes terroristes.

En raison de l'interconnectivité croissante, les infrastructures essentielles de l'information sont désormais exposées à des menaces et à des vulnérabilité de plus en plus nombreuses et de plus en plus diverses qui posent de nouveaux problèmes de sécurité. L'utilisation par des acteurs étatiques et non étatiques des nouvelles technologies de l'information et des communications à des fins incompatibles avec la paix et la sécurité internationales est un problème grave qui nécessite les efforts de tous les États.

L'utilisation clandestine et illégale par des individus, des organisations et des États, des systèmes informatiques d'autres nations pour attaquer des pays tiers sont susceptibles de déclencher de graves conflits. Le seul moyen de prévenir et de combattre ces menaces passe par une coopération conjointe entre tous les États afin d'assurer la cybersécurité et de protéger les infrastructures essentielles en appuyant les efforts nationaux visant à renforcer les capacités humaines, en créant davantage de possibilités d'emploi et d'apprentissage et en améliorant les services publics et la qualité de vie de la population. Nous devons parvenir à un instrument international juridiquement contraignant au sein du système des Nations Unies, qui réglemente l'utilisation des technologies de l'information et des communications et veille à ce qu'elles soient utilisées dans le respect du droit international et en particulier de la Charte des Nations Unies.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de l'Iraq.

M. Alhakim (Iraq) (*parle en arabe*) : Tout d'abord, qu'il me soit permis de remercier l'Ukraine et son Ministre des affaires étrangères d'avoir convoqué cet important débat public sur la protection des infrastructures essentielles. L'Iraq accueille également avec satisfaction l'adoption aujourd'hui de la résolution 2341 (2017), dont elle a été coauteur.

Nous ne devons pas imputer le terrorisme à une religion, une culture, une nationalité ou une

région géographique, comme cela a été confirmé par de nombreuses résolutions du Conseil de sécurité, dont la plus récente est la résolution 2253 (2015). Les défis posés par des organisations terroristes telles que les gangs terroristes de l'État islamique d'Iraq et du Levant (EIIL), tiennent à leur forte capacité d'organisation, ce qui leur permet de perpétrer dans le cyberespace des attentats terroristes qui ont un impact physique direct sur les infrastructures critiques. Ces attaques détruisent ces infrastructures et entravent leur fonctionnalité, ce qui cause de graves préjudices. Les gangs de l'EIIL s'emploient à renforcer leurs capacités organisationnelles et leurs stratégies visant à recruter dans les pays développés des partisans qui ont bénéficié d'un enseignement dans des universités occidentales prestigieuses. Ces recrues très éduquées permettent aux organisations terroristes de mener des attaques cybernétiques transfrontalières qui échappent à toutes restrictions nationales, créant ainsi une réalité où il n'existe effectivement aucune frontière.

Il est extrêmement important de renforcer la coopération internationale dans le domaine de la lutte contre le terrorisme, en particulier parce que l'EIIL commet ses crimes par le biais de réseaux décentralisés. Ses gangs ont augmenté leurs capacités techniques aux fins de l'exécution de cyberattaques et recrutent les terroristes étrangers qui ont des compétences avancées pour effectuer ces attaques complexes.

Parmi les tendances les plus importantes qui peuvent être observées dans le fonctionnement des organisations terroristes, en particulier les gangs terroristes de Daech, est le ciblage continu des infrastructures essentielles en Iraq, y compris les ponts, les lignes électriques, les tours de télécommunications et les oléoducs. Le terrorisme a eu des répercussions sur de nombreux projets qui constituent l'épine dorsale de l'infrastructure iraquienne. Les terroristes ont également brûlé des monuments, des mosquées et des universités. Ces attaques terroristes ont augmenté le coût des projets de développement en raison du coût croissant des mesures de sécurité nécessaires pour protéger les sites de construction. Le ciblage des installations pétrolières et des raffineries dans les régions soumises à de nombreux attentats terroristes est l'une des attaques les plus graves contre l'économie et l'infrastructure de l'Iraq car le pays dépend essentiellement des recettes pétrolières.

La libération des villes iraquiennes précédemment contrôlées par les gangs de Daech se fait généralement à grand coût économique. Lors de la bataille pour reprendre possession de Mossoul, les gangs de l'EIIL ont posé des mines et des engins explosifs dans des maisons individuelles et dans des bâtiments publics, ainsi que sur des ponts, afin de les détruire et d'empêcher les forces de sécurité d'avancer vers ces villes. Ces difficultés se sont accrues avec la diminution du prix du pétrole sur le marché mondial, puisque les recettes pétrolières constituent l'élément principal du budget national de l'Iraq.

Pour conclure, mon gouvernement est vivement reconnaissant du rôle actif et des efforts de la coalition mondiale, de la Mission d'assistance des Nations Unies pour l'Iraq et d'autres organisations internationales, en particulier du Programme des Nations Unies pour le développement. Nous demandons à la communauté internationale de consentir des efforts supplémentaires pour reconstruire les zones libérées de mon pays, rétablir la stabilité et remettre en état nos infrastructures, notamment les écoles et les hôpitaux.

Le Président (*parle en anglais*) : Je donne la parole au représentant du Bangladesh.

M. Bin Momen (Bangladesh) (*parle en anglais*) : Nous remercions la présidence ukrainienne d'avoir organisé le présent débat public, et les intervenants de leurs exposés instructifs.

Le Bangladesh s'associe à la déclaration que fera le représentant de la République bolivarienne du Venezuela au nom du Mouvement des pays non alignés.

La résolution 2341 (2017), adoptée aujourd'hui, aidera à donner un nouvel élan à la protection des infrastructures essentielles contre les attaques terroristes. La résolution a été élaborée à un moment où, selon certaines informations, des terroristes font des tentatives de plus en plus nombreuses et complexes pour avoir accès aux infrastructures essentielles et les attaquer. La nécessité d'effectuer des analyses relatives à la sécurité des infrastructures essentielles est devenue d'autant plus importante, afin de renforcer la résilience et l'état de préparation, à la suite de certains attentats terroristes récents dans des aéroports internationaux et du ciblage d'autres infrastructures essentielles.

Le présent débat public a été utile pour mettre en lumière un certain nombre d'initiatives nationales et régionales actuelles, en particulier dans le contexte d'une interdépendance croissante entre les différents secteurs des infrastructures essentielles. Nous prenons note du travail en cours dans ces différents secteurs, notamment l'industrie, la gestion de la chaîne des

approvisionnements, les services publics, les transports transfrontaliers et le cyberespace. Ce travail doit constituer un ensemble utile de bonnes pratiques et aider à enrichir le travail législatif qui doit encore être accompli au niveau international, en particulier sur la cybersécurité. Les conséquences environnementales des attaques terroristes contre les infrastructures essentielles, notamment dans les centres densément peuplés des villes, soulignent la complexité des défis que nous devons relever.

Au Bangladesh, nos autorités compétentes continueront d'étudier dans le détail la résolution 2341 (2017), afin de recenser les lacunes existantes, les difficultés et les points forts au niveau national, en vue de remédier aux éventuelles vulnérabilités de nos infrastructures essentielles face aux attaques terroristes. Nous restons conscients de la nature très largement transnationale de la plupart des menaces contre les infrastructures essentielles, et nous avons l'esprit ouvert au renforcement de la coopération régionale et sous-régionale à cet effet. Dans certains domaines, nous souffrons de contraintes évidentes en matière de capacités, et de nombreux États Membres dans une situation comparable continueront de dépendre de l'Organisation des Nations Unies, en tant que premier intervenant ainsi que prestataire d'une assistance régulière en matière de renforcement des capacités, y compris pour les mesures à prendre face aux imprévus.

Dans le contexte du renforcement de notre état de préparation au niveau national, nous avons travaillé avec l'Équipe spéciale de lutte contre le terrorisme et plusieurs entités compétentes de l'Organisation des Nations Unies dans les domaines de la sécurité nucléaire, de la sécurité maritime et aéronautique, de la lutte contre le financement du terrorisme, et de la cybersécurité. Ce travail de renforcement des capacités a été essentiel pour que nos organismes intéressés et d'autres parties prenantes deviennent plus conscients des cadres juridiques et normatifs internationaux existants. Cela a également aidé à dresser une carte des différents volets – qui se renforcent mutuellement – du travail de diverses entités qui pourraient bénéficier d'un resserrement de la coordination et de la cohérence. Nous attendons avec intérêt de tirer parti d'un tel travail, en vue d'élaborer une approche stratégique nationale concernant l'anticipation et la prévention des attaques et menaces terroristes contre les infrastructures essentielles. Le travail accompli pour protéger les infrastructures contre les actes criminels et les risques naturels doit également contribuer à ces efforts.

La primauté de l'évaluation des risques, de l'alerte rapide et du partage d'informations pour la protection des infrastructures essentielles et des civils ne saurait être trop soulignée. Le Bangladesh demeure un partenaire fiable de la communauté internationale dans le domaine du partage des informations, conformément à l'approche tolérance zéro de notre Première Ministre à l'égard du terrorisme, sous toutes ses formes et dans toutes ses manifestations. Nous exhortons le Comité contre le terrorisme, y compris sa Direction exécutive, à entreprendre des consultations avec les protagonistes nationaux et régionaux, tout en faisant le bilan des efforts des États Membres, afin de se fonder sur des données factuelles et bien attestées.

L'importance vitale d'établir des partenariats entre les secteurs public et privé a été soulignée par presque toutes les délégations. Le Bangladesh souhaite vivement participer à des instances internationales et régionales compétentes, qui rassemblent des représentants des secteurs public et privé pour promouvoir des synergies grâce à leur travail, et en tirer des enseignements. Nous reconnaissons les avantages éventuels du développement de certaines normes internationales de préparation aux situations d'urgence, que le secteur privé pourrait être tenu de respecter.

Dans le contexte de menaces terroristes en évolution rapide, nous soulignons la nécessité de faciliter le partage des connaissances et les transferts de technologies, dans un esprit de coopération internationale efficace et de partenariat. Si tous les États Membres doivent continuer d'assumer leur responsabilité principale de contrer les menaces terroristes contre les infrastructures majeures, une grande partie de notre succès collectif dépendra de façon cruciale du soutien, en fonction des besoins, qui doit être mis à la disposition des pays en développement et des pays les moins avancés par les partenaires de développement concernés, y compris l'Organisation des Nations Unies.

Le Président (*parle en anglais*) : Je donne maintenant la parole à la représentante du Pakistan.

Mme Lodhi (Pakistan) (*parle en anglais*) : Je tiens tout d'abord à remercier la délégation de l'Ukraine d'avoir convoqué le présent débat sur une question d'une grande importance.

Parmi la myriade de menaces qui mettent en danger la sécurité mondiale, le terrorisme est devenu l'un des défis les plus complexes et les plus imposants de notre époque. Notre dépendance à l'égard des

infrastructures essentielles en fait une cible de choix pour les terroristes de tout acabit. Les attaques terroristes contre les infrastructures visent à bouleverser les vies, à semer une peur généralisée et le chaos, à retarder le développement socioéconomique et à entraver la coopération économique régionale. Les avancées dans le domaine des technologies de la communication, qui rendent le monde interdépendant et interconnecté, et l'utilisation accrue de communications chiffrées par des organisations terroristes telles que Daech ont amplifié la menace d'un attentat terroriste contre des pôles financiers et énergétiques. La détermination nationale et l'action collective sont nécessaires pour protéger les infrastructures, qui sont essentielles pour le bien-être et le progrès de nos peuples.

Mon pays a affronté et combattu le terrorisme pendant plusieurs décennies, avec courage et conviction. Notre résilience a été mise à l'épreuve à maintes reprises, de l'attentat barbare contre l'hôtel Marriott à Islamabad, en 2008, à la destruction de matériel militaire au cours de l'attaque contre une base de l'armée de l'air à Kamra, en 2012, ainsi qu'à l'attentat contre l'aéroport de Karachi en 2014. Ces attaques visaient à détruire et à perturber les vies de mes concitoyens, à affaiblir nos forces de défense et à démoraliser la nation, mais elles n'ont fait que renforcer la détermination de notre peuple de poursuivre ses efforts afin d'éliminer ce fléau.

Ces quatre dernières années, le Pakistan a adopté une stratégie multidimensionnelle. Une opération dirigée par les militaires, appelée Zarb-e-Azb, a réussi à détruire les infrastructures terroristes, et un plan d'action national, sous-tendu par un consensus national solide, a visé à contrer efficacement les discours des organisations terroristes et extrémistes. Cette approche globale a réussi à expulser des organisations terroristes de notre territoire et a beaucoup réduit leur capacité de mener des attaques meurtrières, comme le démontre la diminution spectaculaire du nombre de celles-ci, en dépit du lâche attentat terroriste de ce matin à Lahore. Cependant, le Pakistan continue actuellement d'être confronté à des terroristes soutenus de l'extérieur, dont le nombre augmente. L'une de leurs cibles principales, ce sont les infrastructures majeures que nous construisons actuellement au Pakistan. Leur objectif est de saper nos réalisations et notre stabilité économiques.

La maîtrise par l'État des systèmes d'infrastructure et son rôle s'agissant de déterminer les modalités de protection efficace des infrastructures sont fondamentaux. La diversité des menaces exige une riposte cohérente par toutes les parties prenantes nationales, fondée sur l'environnement propre à chaque pays. Les organisations internationales et régionales et la coopération régionale restent également vitales pour contrecarrer la menace du terrorisme. Au niveau régional, le partage de l'information et des évaluations des menaces, ainsi que la gestion efficace des frontières et la mise en commun des meilleures pratiques, peuvent considérablement renforcer les capacités nationales de dissuasion et de victoire sur le terrorisme.

C'est dans cet esprit que mon pays a adhéré à la Convention régionale de l'Association sud-asiatique de coopération régionale (ASACR) sur la répression du terrorisme. Malheureusement, en tant qu'organisation, l'ASACR est devenue victime des desseins hostiles de certains de nos voisins, ce qui limite considérablement la capacité de notre région à lutter contre les multiples problèmes auxquels elle est confrontée, notamment le terrorisme. Bien que demeurant attaché au renforcement de la coopération régionale en matière de lutte contre le terrorisme, le Pakistan continue de subir des attaques terroristes régionales soutenues par des forces régionales. Nous sommes déterminés à repousser ce terrorisme d'État, et nous en sommes pleinement capables.

L'ONU peut et doit jouer un rôle dans le renforcement de la capacité des États Membres à lutter contre le terrorisme. Le Groupe de travail sur la protection des infrastructures critiques de l'Équipe spéciale de lutte contre le terrorisme joue un rôle positif à cet égard. L'ONU sert également de plateforme pour aider les États Membres à identifier les menaces et risques potentiels auxquels sont exposées leurs installations et à élaborer des stratégies et des partenariats cohérents aux fins de l'exécution de ces plans.

Dans le cadre de la lutte contre la menace terroriste, il est essentiel que la communauté mondiale analyse et comprenne le phénomène du terrorisme dans toutes ses complexités. La campagne mondiale de lutte contre le terrorisme ne saurait être réduite à un slogan diffamatoire visant l'islam, ou toute autre religion ou race. Il importe également d'examiner les raisons pour lesquelles, en dépit de la campagne mondiale de lutte contre le terrorisme, la menace continue d'évoluer et d'émerger sous des formes nouvelles et sur la base d'idéologies nouvelles et toujours plus virulentes et toxiques, sur des superficies régionales de plus en plus vastes, posant une menace omniprésente à la paix et à la sécurité internationales et nationales.

Le Pakistan reste convaincu que pour vaincre et éliminer le terrorisme, il est essentiel de lutter contre les causes profondes qui créent des recrues pour les terroristes : les conflits internes et interétatiques non réglés, le recours illégal à la force, les agressions et les interventions extérieures, l'occupation étrangère, le déni du droit à l'autodétermination, l'injustice politique et économique, ainsi que la marginalisation et la mise à l'écart de certaines communautés et de certains groupes. Ce n'est qu'en luttant contre ces causes profondes que la communauté internationale parviendra à éroder l'attrait des discours haineux et hostiles qui fournissent au terrorisme l'oxygène nécessaire pour lui permettre d'exister et de se développer.

Le Président (*parle en anglais*) : Je donne maintenant la parole à M. Meszaros.

M. Meszaros (*parle en anglais*) : Les alliés de l'Organisation du Traité de l'Atlantique Nord (OTAN) et la communauté internationale dans son ensemble sont confrontés à un grand nombre de problèmes liés au terrorisme qui menacent directement la sécurité de nos populations ainsi que la stabilité et la prospérité internationales. Nous avons été frappés par de terribles attaques terroristes sur nos territoires et dans nos villes. Compte tenu de l'évolution des conditions de sécurité, l'OTAN est en train de renforcer ses capacités de dissuasion et de défense. Cela signifie qu'il faut investir dans le renforcement des capacités militaires, mais également renforcer la résilience des pays face à toutes les menaces, en particulier celles qui visent directement les cibles vulnérables, notamment nos populations civiles, nos infrastructures essentielles, nos réseaux informatiques et nos fonctions gouvernementales essentielles. C'est pourquoi au Sommet de Varsovie organisé par l'OTAN, les chefs d'État et de gouvernement se sont engagés à renforcer la résilience dans ces domaines et dans d'autres domaines critiques.

Plus important encore, en ce qui concerne la protection des infrastructures essentielles, les membres de l'OTAN ont décidé de répondre aux besoins en matière de résilience dans sept secteurs : la continuité de l'État, l'approvisionnement en énergie, l'approvisionnement civil, les systèmes de transport civils, les services de communication civils, l'approvisionnement en vivres et en eau et la capacité à gérer les événements provoquant un grand nombre de victimes et les mouvements de réfugiés à grande échelle. Ces exigences définissent le niveau de résilience que doivent atteindre nos alliés pour pouvoir lutter contre toutes les menaces. Les pays membres de l'OTAN font maintenant le nécessaire pour répondre à ces besoins.

Pour l'OTAN, le renforcement de la résilience est conforme à l'esprit de l'article 3 du Traité fondateur de Washington, en vertu duquel tout allié est tenu de faire le nécessaire pour résister à une attaque. Toutefois, à une époque marquée par l'interconnexion mondiale, nous notons que notre propre résilience est directement liée à celle de nos voisins. C'est pourquoi les activités de l'OTAN visant à renforcer la résilience et à protéger les infrastructures essentielles couvrent également ses partenaires. Si nos partenaires sont plus résilients, l'OTAN sera plus en sécurité.

L'engagement pris au Sommet de Varsovie a donc mis en exergue la nécessité de fournir un appui constant à nos partenaires et d'améliorer la coopération avec d'autres organisations internationales afin d'éliminer les vulnérabilités et de renforcer la sécurité de l'Alliance, du voisinage de l'OTAN et du système international en général. Aucune entité n'est dotée de tous les moyens nécessaires pour assurer sa résilience.

En conséquence, nous collaborons avec l'Union européenne pour renforcer la résilience face aux menaces hybrides, et nous proposons une assistance au renforcement des capacités à nos partenaires d'Europe de l'Est, d'Europe du Sud-Est, d'Afrique du Nord et du Moyen-Orient, en particulier en vue de créer des systèmes efficaces de gestion des crises et en matière de formation. Nous promouvons ces activités en collaborant avec les pays partenaires, le secteur privé et nos homologues de l'Union européenne pour définir les exigences minimales en matière de résilience afin de garantir la transparence et la compatibilité et de promouvoir un sentiment de responsabilité partagée.

L'OTAN peut servir de plateforme pour permettre à ses alliés et partenaires de partager leurs connaissances spécialisées et leurs pratiques optimales, et elle peut également proposer des formations et mener des activités de sensibilisation dans les domaines de la protection des infrastructures essentielles et de la lutte contre le terrorisme en général. Nous sommes disposés à partager nos pratiques optimales et les enseignements retenus, le cas échéant, avec les organes compétents de l'ONU, en particulier l'Équipe spéciale de lutte contre le terrorisme et le Groupe de travail qui dépend d'elle. Compte tenu de l'interconnexion avec d'autres acteurs, nous estimons que la résilience et la protection des infrastructures essentielles sont une responsabilité commune, et nous sommes prêts à mettre les données

d'expérience et les connaissances spécialisées de l'OTAN au service des initiatives internationales visant à renforcer la résilience.

Le Président (*parle en anglais*) : Je remercie M. Meszaros de son exposé.

Je donne maintenant la parole au représentant du Koweït.

M. Alotaibi (Koweït) (*parle en arabe*) : Je vous félicite, Monsieur le Président, de votre accession à la présidence du Conseil de sécurité. Nous nous félicitons de l'adoption de la résolution 2341 (2017) ce matin. Je saisis cette occasion pour saluer la délégation suédoise, qui a assuré la présidence du Conseil de sécurité en janvier.

Pour en venir au sujet du présent débat, je vous remercie de la note de cadrage élaborée par votre délégation (S/2017/104, annexe), et je remercie les intervenants de leurs exposés instructifs.

Le terrorisme est un danger qui menace la paix et la sécurité internationales et cible des civils innocents – femmes, enfants et personnes âgées – ainsi que des infrastructures civiles essentielles. En 2015, le Koweït a été victime d'actes de terrorisme qui ont ciblé des structures religieuses et ont fait une grand nombre de morts et de blessés. En 1990, alors que notre pays était sous occupation iraquienne, des puits de pétrole ont été pris pour cible, ce qui a détruit notre environnement. C'est pourquoi nous avons demandé que le 6 novembre soit proclamé Journée internationale pour la prévention de l'exploitation de l'environnement en temps de guerre et de conflit armé.

Le Koweït a pris de nombreuses mesures pour protéger ses installations. Nous appuyons les efforts que déploie la communauté internationale dans sa lutte contre Daech. Nous condamnons le terrorisme sous toutes ses formes et dans toutes ses manifestations. Les actes de terrorisme sont injustifiables et ne sauraient être reliés à une religion ou une nationalité en particulier. La lutte contre le terrorisme nécessite d'accentuer les efforts internationaux tout en respectant les droits de l'homme, la primauté du droit, les principes de bonne gouvernance et de coexistence pacifique des religions ainsi que les symboles religieux. À cet égard, nous insistons sur la nécessité de mettre en œuvre les résolutions 1373 (2001), 1963 (2010), 2129 (2013) et 2322 (2016) et toutes les autres résolutions pertinentes.

Nous soulignons également la nécessité de mettre en œuvre la Stratégie antiterroriste mondiale des Nations Unies et d'appuyer la Direction exécutive du Comité contre le terrorisme dans cette optique. Nous soulignons par ailleurs l'importance de l'assistance technique et du renforcement des capacités en vue de protéger les infrastructures essentielles tout en renforçant le dialogue entre les pays et les organisations régionales et internationales afin de mettre en commun les données d'expérience et les pratiques optimales pertinentes. Nous tenons en outre à souligner l'importance de la coopération internationale, notamment avec INTERPOL, sur la base de l'échange de l'information et des connaissances spécialisées, pour lutter contre le terrorisme et améliorer la protection des infrastructures essentielles.

Nous encourageons tous les États Membres à tirer parti des travaux réalisés dans ce domaine par les programmes et les institutions spécialisées des Nations Unies, ainsi que par les organisations régionales et internationales. Les infrastructures essentielles sont une cible de choix pour les terroristes dans le monde entier, et la connectivité entre ces infrastructures les rend plus vulnérables aux attaques. Les attaques contre les installations ayant recours aux technologies de l'information et des communications peuvent être un facteur aggravant de risque. C'est pour cette raison que les gouvernements doivent coopérer pour formuler des plans d'intervention d'urgence.

Ici, nous voudrions rappeler la résolution 2286 (2016) qui appelle à la protection des installations médicales, des acteurs humanitaires et de leur matériel en période de conflit armé. Cette résolution est pleinement conforme au droit international humanitaire et au droit des droits de l'homme.

S'il est vrai que le terrorisme se poursuit sans relâche et que l'EIIL continue de commettre des actes ignobles, en plus des actes perpétrés par Boko Haram, les Chabab et le Front el-Nosra au Yémen, en Syrie, en Iraq, en Libye et en Somalie, ces groupes continuent de perdre du terrain et de l'influence dans de nombreuses régions du monde, comme le Secrétaire général l'indique dans son rapport publié sous la cote S/2017/97. Nous voudrions souligner l'importance d'une action collective en vue de la reconstruction d'infrastructures essentielles. À cet égard, le Koweït continue d'apporter son aide aux déplacés et aux réfugiés et d'apporter son appui en vue de la reconstruction des infrastructures essentielles détruites par le terrorisme pour que les

civils puissent reprendre une vie normale, notamment les hôpitaux et les écoles qui ont été touchés, ainsi que d’autres installations.

Enfin, nous voudrions réitérer notre position ferme, en condamnant le terrorisme, et souligner l’importance du droit international, des quatre Conventions de Genève et des résolutions pertinentes du Conseil de sécurité, ainsi que de la coopération internationale par l’entremise de l’ONU pour contrer cette menace.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de la République bolivarienne du Venezuela.

M. Ramírez Carreño (République bolivarienne du Venezuela) (*parle en espagnol*) : Pour faciliter le bon déroulement de la présente séance, je vais donner lecture d’une version abrégée de la déclaration que la République bolivarienne du Venezuela a l’honneur de prononcer au nom du Mouvement des pays non alignés. Le texte intégral sera publié sur le site Web de la présidence du Bureau de coordination du Mouvement. En outre, je ferai quelques brèves observations sur cette question à titre national.

Tout d’abord, nous voudrions saluer respectueusement, au nom des États membres du Mouvement, le Ministre des affaires étrangères de l’Ukraine, S. E. M. Pavlo Klimkin, et exprimer nos meilleurs vœux à sa délégation et à l’Ambassadeur Volodymyr Yelchenko pour une présidence du Conseil couronnée de succès ce mois-ci. De même, nous voudrions saluer la diligence avec laquelle la délégation suédoise, sous la houlette de l’Ambassadeur Skoog, a dirigé les travaux du Conseil en janvier.

Lors du dix-septième sommet du Mouvement des pays non alignés, tenu en Septembre 2016 sur l’île de Margarita au Venezuela, les chefs d’État et de gouvernement ont réitéré que le terrorisme constituait une des plus graves menaces à la paix et à la sécurité internationale et ont réaffirmé que tous les actes terroristes sont criminels et injustifiables, quelles qu’en soient les motivations, où qu’ils soient commis et quels qu’en soient les auteurs, puisqu’ils constituent une violation flagrante du droit international.

Ils ont réaffirmé par ailleurs que le terrorisme ne peut pas ni ne saurait être associé à une religion, à une nationalité, à une civilisation ou à un groupe ethnique, et que ces attributions ne sauraient être utilisées pour justifier le terrorisme ou les mesures de lutte contre le terrorisme, y compris, entre autres, la mise au point de profils de suspects et l’invasion de la vie privée.

Les attaques terroristes les plus récentes, notamment celles perpétrées par Daech, prouvent que le monde entier est désormais vulnérable face à ce fléau et au phénomène des combattants terroristes étrangers. Dans cet ordre d’idées, il convient de noter que la destruction des infrastructures physiques et économiques des États, y compris les infrastructures essentielles, a toujours revêtu un intérêt particulier pour les groupes terroristes. Il faut également mentionner le climat de terreur que de telles attaques crée au sein du grand public ainsi que la grande publicité qui en est faite à l’échelle mondiale.

La protection des infrastructures essentielles joue un rôle important dans les efforts visant à prévenir et à combattre le terrorisme et pourrait être intégrée dans les plans nationaux visant à prévenir et à combattre ce fléau, le cas échéant. Par conséquent, le renforcement de la coopération internationale et régionale, notamment en adoptant des mesures adéquates et efficaces pour éliminer ce fléau et en établissant des partenariats appropriés, revêt la plus haute importance.

À cet égard, les États membres du Mouvement sont d’avis que la lutte contre le terrorisme doit être menée conformément aux instruments internationaux et régionaux portants sur cette, notamment les buts et principes énoncés dans la Charte des Nations Unies, et dans le plein respect des droits de l’homme et des libertés fondamentales, conformément à l’état de droit et aux obligations découlant du droit international.

En outre, la fourniture d’une assistance technique, sur demande, en vue du renforcement des capacités et de la mise en place d’infrastructures, de mécanismes et de processus, notamment par l’échange d’informations, de meilleures pratiques et l’identification de domaines vulnérables dans lesquels des améliorations s’imposent, est d’une importance capitale en matière de lutte contre le terrorisme. À cet égard, l’appui et les ressources que le Centre des Nations Unies pour la lutte contre le terrorisme peut fournir aux États Membres, sur demande et conformément à son mandat, seraient très utiles dans le cadre des efforts qu’ils déploient pour prévenir et combattre le terrorisme. Il en va de même des compétences spécialisées qui pourraient être mises à leur disposition, par exemple par le Groupe de travail sur la protection des infrastructures critiques, y compris Internet, les cibles vulnérables et la sécurité du tourisme de l’Équipe spéciale de lutte contre le terrorisme.

Pour terminer, le Mouvement des pays non alignés réaffirme son plein engagement en faveur de la lutte contre le terrorisme. Nous insistons sur le fait qu'il est essentiel que ces efforts soient déployés de manière franche, décisive et coordonnée, notamment grâce à la mise en œuvre intégrale et équilibrée des résolutions pertinentes de l'ONU et de la Stratégie antiterroriste mondiale des Nations Unies. De même, l'adoption à l'avenir d'une convention générale sur le terrorisme international sous l'égide de l'ONU permettrait de renforcer la coopération multilatérale dans ce domaine.

Qu'il me soit permis de faire quelques observations à titre national.

Nous voudrions souligner que le Venezuela a exprimé à maintes reprises sa position concernant la menace que représente le terrorisme sous toutes ses formes et dans toutes ces manifestations au sein des instances qui s'occupent de ce problème en condamnant fermement les actes terroristes, quelles qu'en soient les motivations et quels qu'en soient les auteurs, étant donné leurs incidences néfastes sur la paix et la sécurité internationales, les droits de l'homme et le développement. En outre, durant notre mandat au Conseil de sécurité, nous n'avons cessé d'appeler au renforcement de la coopération internationale pour prévenir, combattre et éliminer ce phénomène odieux, tout en insistant sur la nécessité d'adopter une approche holistique face au problème du terrorisme.

Notre pays se félicite de l'adoption, aujourd'hui, de la résolution 2341 (2017), ainsi que des résolutions adoptées par le Conseil l'an dernier, notamment la résolution 2286 (2016) portant sur la protection des hôpitaux et du personnel humanitaire dans les situations de conflit.

Nous sommes convaincus que pour lutter efficacement contre le terrorisme,il faut renoncer à la politique de deux poids deux mesures et à d'autres approches erronées qui font que les efforts conjoints des États Membres n'aboutissent pas à des résultats concrets en faveur de la paix et de la sécurité internationales. Malheureusement, ces dernières années, le terrorisme a été stimulé par l'interventionnisme et les agressions armées de puissances étrangères – dont ont été victimes des pays frères comme l'Iraq, la Libye et la Syrie, entre autres – visant à renverser des gouvernements légitimement établis, provoquant ainsi l'effondrement du tissu institutionnel de ces États et les rendant vulnérables à la violence et aux discours de haine et d'intolérance promus par les groupes terroristes.

Nous ne pouvons pas non plus passer sous silence les actes de terrorisme perpétrés par des acteurs étatiques, comme la terreur semée par l'agression militaire israélienne contre la population palestinienne de Gaza depuis près de trois ans, causant des pertes en vies humaines, notamment des femmes et des enfants, et la destruction d'infrastructures critiques essentielles pour remédier à la situation humanitaire dramatique de la population palestinienne résultant de l'imposition d'un blocus illégal qui dure depuis 2007. Les hôpitaux, les services d'approvisionnement en eau potable, les voies d'accès et les écoles, entre autres, ont été bombardés délibérément de façon aveugle et systématique au cours du conflit armé pour punir et agresser l'ensemble de la population civile. Les séquelles de la destruction demeurent présentes et se manifestent dans une population en proie au désespoir confrontée à un processus de reconstruction entravé par les politiques appliquées par les autorités israéliennes, qui bloquent l'accès des matériaux et des services.

C'est pourquoi lorsque nous parlons de prévention et de lutte contre la barbarie terroriste, nous devons garder à l'esprit que les politiques d'intervention et d'occupation étrangère sont une cause fondamentale de l'instabilité et créent donc des conditions favorables à l'émergence et à l'expansion d'acteurs non étatiques violents qui se transforment en groupes terroristes. C'est pourquoi nous demandons que cessent les agressions armées et l'ingérence dans les affaires intérieures des pays qui sont des pratiques illégales de politique étrangère utilisées comme instruments d'affirmation de la puissance au niveau international.

De même que toute discussion sincère sur la portée de la Stratégie antiterroriste implique nécessairement de reconnaître le problème que représente actuellement le financement, la formation et la fourniture d'armes assurés par des puissances étrangères à des acteurs non étatiques violents.

Ces facteurs ont eu une incidence profonde sur la paix, la stabilité et le développement en Syrie, en Iraq, en Libye et dans d'autres pays touchés par le terrorisme, avec les conséquences que l'on sait, comme la destruction d'infrastructures critiques, notamment de l'appareil de production et du patrimoine culturel, l'utilisation d'armes chimiques contre la population civile et les violations massives des droits de l'homme et du droit international humanitaire. Ces actes scandaleux sont tous constitutifs de crimes de guerre.

La lutte contre le terrorisme en général et la protection des infrastructures critiques en particulier requièrent de la communauté internationale qu'elle mette en œuvre une stratégie antiterroriste mondiale inspirée de la résolution 70/288 de l'Assemblée générale, qui soit assortie, d'une part, d'un véritable plan de coopération fondé sur le droit international et, d'autre part, d'une impulsion aux politiques publiques nationales de prévention et de lutte contre les actes terroristes, qui doivent être conçues et mises en œuvre dans le strict respect de l'état de droit, notamment des droits de l'homme, et ce sans discrimination ou préjugés à caractère ethnique ou religieux pouvant constituer un terreau fertile au ressentiment et à l'extrémisme violent promus par les groupes terroristes. À cet égard, nous exprimons notre solidarité avec les pays dont on veut inscrire les citoyens sur des listes restrictives uniquement en raison de leur origine nationale et de leur religion. Nous estimons que cette approche n'est pas le moyen approprié de contrer la menace terroriste.

Enfin, nous réitérons que c'est à l'ONU et à ses États Membres qu'il incombe de veiller à l'application effective et opportune des résolutions de l'Assemblée générale et du Conseil de sécurité ainsi que des obligations découlant des traités internationaux pertinents en vue de faire face à ce phénomène mondial et de protéger les infrastructures critiques et la population contre la violence aveugle des groupes terroristes.

Le Président (*parle en anglais*) : Je donne maintenant la parole à la représentante de la Jordanie.

Mme Bahous (Jordanie) (*parle en arabe*) : Je voudrais tout d'abord féliciter l'Ukraine de son accession à la présidence du Conseil de sécurité pour ce mois et lui souhaiter plein succès. Je la félicite aussi d'avoir organisé cette importante séance thématique. Je remercie aussi tous les intervenants de leurs exposés, et nous saluons, nous aussi en Jordanie, l'adoption de la résolution 2341 (2017), qui vient sans nul doute renforcer l'action menée actuellement pour lutter contre le terrorisme d'une manière générale et, en particulier, aider à mieux protéger les infrastructures critiques contre la menace terroriste.

Le terrorisme continue de constituer l'une des menaces les plus graves à la paix et à la sécurité internationales. Les horribles attaques terroristes menées par des groupes terroristes comme Daech dans différents pays du monde et la propagation du phénomène des combattants terroristes étrangers attestent du caractère universel du terrorisme qui, outre les civils innocents, ciblent maintenant les installations et les infrastructures critiques. En effet, le ciblage des sites touristiques, des aéroports, des ports, des installations pétrolières, des centrales électriques, des réservoirs d'eau, des systèmes électroniques des entreprises financières comme les banques et les grands projets et les sites appartenant au patrimoine, ainsi que la destruction des principales voies de communication et des ponts se répercutent négativement et de façon directe sur les autres secteurs et services, suscitent la crainte et font perdre confiance aux citoyens dans leurs institutions nationales. C'est pourquoi nous ne pouvons séparer la protection des infrastructures critiques du cadre général de la lutte contre le terrorisme, et nous devons veiller à ce que la protection de ces infrastructures soit une partie intégrante de tous les efforts visant à améliorer la sécurité et la protection des cibles potentielles.

Cela doit se faire par la mise en œuvre la Stratégie antiterroriste mondiale des Nations Unies ainsi qu'en garantissant et en développant des stratégies antiterroristes nationales pour y inclure les infrastructures critiques. Il importe à cet égard d'insister sur la nécessité que la communauté internationale renforce la coopération internationale et régionale en réponse à cette menace en vue de préserver les vies et de protéger plus efficacement les infrastructures critiques, et ce en allant de l'avant dans la mise en place des mécanismes susceptibles de renforcer les capacités des pays pour les aider à protéger leurs infrastructures nationales, en mettant en commun les données d'expérience des pays, et en améliorant l'utilisation des systèmes de partage des renseignements fournis par les institutions des Nations Unies et d'autres organisations internationales comme INTERPOL.

À cet égard, nous réaffirmons notre appui à la proposition du Secrétaire général tendant à la création d'un bureau chargé de la lutte contre le terrorisme, et espérons que cette proposition sera une première étape pour unir et rendre plus cohérents les efforts des Nations Unies visant à lutter contre le terrorisme, notamment en renforçant les capacités, en améliorant la gestion des ressources allouées et en veillant à une mise en œuvre équilibrée et efficace de la Stratégie antiterroriste mondiale des Nations Unies. Partant, nous réaffirmons qu'il importe que le Groupe de travail sur la protection des infrastructures critiques, y compris Internet, les cibles vulnérables et le sécurité du tourisme continue d'œuvrer pour aider les pays à mettre en œuvre les dispositions de la Stratégie antiterroriste mondiale et à établir des partenariats entre les secteurs public-privé, de façon à

assurer un équilibre entre les questions économiques et sécuritaires et à mettre en place un réseau d'experts aux fins du partage de l'information.

Convaincue de ce que l'élément humain reste le facteur le plus important dans la protection des civils ou des infrastructures critiques contre les attaques des groupes terroristes, que ce soit par le biais d'agressions armées ou par l'utilisation des médias sociaux, que la Jordanie a organisé en novembre, en coopération avec l'OTAN, un atelier spécialisé consacré à l'investissement dans les ressources humaines en tant que priorité importante pour lutter contre le terrorisme, en semant les principes de la modération, de la tolérance et de la coexistence pacifique, en particulier dans l'esprit des jeunes.

Pour terminer, je réaffirme que la Jordanie est résolue à demeurer engagée dans la voie qu'elle s'est tracée en matière de lutte contre le phénomène du terrorisme, en s'attaquant à ses causes profondes. La Jordanie a toujours réaffirmé l'importance de la coordination des efforts et de la coopération entre tous les partenaires internationaux face à ce danger, car fermement convaincue que l'élimination du terrorisme ne peut se réaliser qu'au moyen d'une action internationale conjointe et avec une volonté politique sincère de la part de tous les partenaires.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de l'Algérie.

M. Bessedik (Algérie) (*parle en arabe*) : Je voudrais tout d'abord féliciter l'Ukraine de son accession à la présidence du Conseil de sécurité pour ce mois et souhaiter à la délégation ukrainienne plein succès.

Ma délégation s'associe à la déclaration qui a été prononcée par le représentant du Venezuela au nom du Mouvement des pays non alignés.

(*l'orateur poursuit en anglais*)

Je voudrais exprimer la reconnaissance de ma délégation pour la convocation du présent débat public et le choix pertinent du sujet, dont le lien avec la sécurité de mon pays et la vie et le bien-être de mon peuple est d'une importance critique. Nous voudrions saisir cette occasion pour réitérer une fois de plus notre ferme condamnation du terrorisme sous toutes ses formes et dans toutes ses manifestations, quels qu'en soient les motifs, le lieu, le moment et les auteurs. L'Algérie réaffirme également sa détermination à poursuivre la lutte contre le terrorisme et l'extrémisme violent, et continue de mettre en garde contre les idées fausses ou les associations tendancieuses du terrorisme avec certaines religions, civilisations ou zones géographiques.

Selon nous, la lutte contre l'extrémisme violent et le terrorisme doit également inclure la lutte contre la xénophobie et l'islamophobie. L'Algérie est fermement convaincue que la prévention et la lutte contre le terrorisme, y compris la protection des infrastructures essentielles contre les attaques et les menaces terroristes, exigent une grande vigilance et une importante mobilisation. Il est clair que cette lutte ne peut pas se limiter exclusivement à la dimension sécuritaire; elle doit déployer une stratégie nationale cohérente, en amont et en aval.

Dans le domaine spécifique de la protection des infrastructures, l'Algérie a adopté d'importantes mesures qualitatives et consenti des efforts considérables qui ont permis de garantir un environnement sûr pour toutes ses infrastructures publiques et privées. Nous avons gagné notre lutte contre le terrorisme, un fléau qui a touché nombre de nos infrastructures nationales dans les années 90. En outre, nous avons pris des mesures importantes pour assurer la sécurité de nos frontières. La protection de nos infrastructures reste au cœur de notre stratégie nationale : nous mettons ainsi en œuvre des mesures bien coordonnées entre nos différentes forces de sécurité, chacune opérant dans le domaine d'action qui lui est propre.

La résolution 2341 (2017), adoptée plus tôt aujourd'hui, met l'accent sur la coopération internationale et le partage de l'information en temps voulu. Pour sa part, les efforts déployés par l'Algérie pour combattre le terrorisme et améliorer la sensibilisation et la coopération régionales et internationales dans ce domaine sont antérieurs aux grandes attaques terroristes internationales. Dès le début, nous nous sommes efforcés de renforcer les efforts antiterroristes aux niveaux national, régional et international. À cet égard, nous voudrions souligner la nécessité de conjuguer les efforts déployés dans le cadre de la Stratégie antiterroriste mondiale des Nations Unies en améliorant la coopération aux niveaux bilatéral, régional et international, en renforçant les capacités et en mettant en commun les meilleures pratiques et le savoir-faire acquis en matière de lutte contre le terrorisme.

L'Algérie continue de tout mettre en œuvre pour renforcer la coordination et la coopération, en particulier dans la région du Sahel. Le contexte actuel nécessite à la fois la coordination et le renforcement des capacités des

pays de la région sur la base du principe d’appropriation. L’Algérie a engagé une approche concertée au travers de nombreux mécanismes de coopération et contribue à l’approfondissement de la coopération en matière de sécurité entre les pays concernés en coordonnant et en renforçant les mesures de contrôle aux frontières et l’échange de renseignements. Les importantes forces militaires déployées aux frontières de l’Algérie participent aux efforts menés par le Gouvernement pour assurer non seulement notre sécurité nationale, mais aussi celle de nos voisins.

Tout en souscrivant à l’importance de protéger les infrastructures essentielles contre les attaques terroristes, nous sommes fermement convaincus que la lutte contre ce terrible fléau doit être menée tous les jours et dans chaque domaine d’activité, que ce soit politique, institutionnel, économique, culturel, religieux, éducatif ou social. Tout espoir de réussite requiert la participation active de l’ensemble des institutions nationales, de tous les acteurs sociaux et de tous les citoyens.

Enfin, l’Algérie continuera de participer activement à la lutte contre le terrorisme et l’extrémisme violent à tous les niveaux et contribuera de façon constructive aux efforts déployés pour mettre fin au terrorisme, y compris dans le cadre des travaux de l’Assemblée générale.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de la République arabe syrienne.

M. Mounzer (République arabe syrienne) (*parle en arabe*) : Je tiens à vous remercier, Monsieur le Président, d’avoir organisé l’importante séance d’aujourd’hui. Je voudrais affirmer l’appui de la Syrie aux efforts sincères et crédibles déployés par le Conseil de sécurité pour combattre le terrorisme, lesquels attestent de la reconnaissance unanime à l’échelle internationale que le terrorisme est aujourd’hui l’un des plus grands défis au monde et que la communauté internationale doit, par l’intermédiaire de l’ONU et du Conseil de sécurité, jouer son rôle pour coordonner les efforts et la coopération dans le domaine de la lutte contre le terrorisme et l’idéologie extrémiste. La guerre contre le terrorisme n’est pas seulement militaire, c’est aussi une guerre culturelle et de l’information.

Pour la sixième année consécutive, mon pays est la cible de terroristes qui détruisent systématiquement ses installations technologiques et éducatives, ses infrastructures économiques, culturelles et sociales et ses sites historiques. Ces attaques atroces ont pris pour cible des dizaines d’hôpitaux, de bâtiments médicaux, d’écoles, d’universités et d’autres centres de culture et d’éducation, outre la destruction de centrales électriques, de réseaux routiers, de ponts, de chemins de fer, et de réseaux Internet et de télécommunications.

Les groupes armés terroristes, appuyés par des gouvernements bien connus, continuent de commettre leurs actes terribles, dont certains parmi les pires ont visé des sites historiques, religieux et civilisationnels en Syrie, en particulier Palmyre, Alep, Maaloula et Edleb. Ils ont ainsi démoli ou endommagé de nombreux sites et monuments anciens et historiques, des églises, des couvents, des mosquées, des temples, des mausolées et des théâtres, qui ont tous été vandalisés ou détruits de façon barbare. Rien de tout cela n’a quoi que ce soit à voir avec la civilisation humaine. Dès le départ, certains gouvernements se sont associés aux terroristes en Syrie en les finançant et les manipulant, ou ont imposé au peuple syrien des mesures économiques unilatérales et coercitives, ce qui a eu un effet dévastateur sur divers secteurs des services, sur l’économie, l’éducation et la santé, et sur la vie des Syriens. Cela a également réduit la capacité du Gouvernement syrien à répondre aux besoins de ses citoyens. À tout cela, il convient d’ajouter les crimes commis par des groupes terroristes armés contre la Syrie, son peuple et ses infrastructures.

La triste ironie c’est que ce sont précisément les gouvernements qui utilisent l’ONU en tant que forum pour parler de la tragédie humanitaire endurée par le peuple syrien qui ont causé cette tragédie. Dans le cadre de la même politique, ils s’en prennent à l’infrastructure civile syrienne et mènent une ingérence militaire illégale, sous l’appellation de coalition internationale, le tout en violation de la Charte des Nations Unies et du droit international. Ces pays justifient leurs actions par la lutte contre Daech et contre le terrorisme en général, violant ainsi l’Article 51 de la Charte.

Nous avons adressé de nombreuses lettre au Secrétaire général et au Président du Conseil de sécurité contenant des informations et des statistiques précises sur les dommages infligés aux Syriens, à l’infrastructure économique, aux services sociaux, à l’éducation et aux raffineries de pétrole et de gaz. Ces dégâts s’élèvent à plus de 120 milliards de dollars et sont le résultat des exactions et des opérations militaires et aériennes menées par la prétendue coalition internationale, qui a délibérément visé le peuple syrien et son infrastructure.

La République arabe syrienne renouvelle son appel à l'ONU et à la communauté internationale pour que soient mises en œuvre les résolutions du Conseil visant à lutter contre le terrorisme, notamment en mettant fin aux capacités des groupes terroristes qui bénéficient du soutien de certains États qui leur fournissent des financements ainsi que des moyens technologiques et de télécommunications afin de satisfaire des intérêts personnels. Ces gouvernements doivent compenser le peuple syrien et la République arabe syrienne pour les dégâts causés à leur infrastructure. Sans quoi, les résolutions du Conseil et les déclarations des États Membres ne résonneront pas plus loin que cette salle et ne seront que des paroles vides consignées dans les procès-verbaux et autres documents officiels de l'Organisation. Cela enverrait le mauvais message aux terroristes et à ceux qui parrainent le terrorisme.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant des Pays-Bas.

M. van Oosterom (Pays-Bas) (*parle en anglais*) : Je vous remercie, Monsieur le Président, d'avoir organisé l'important débat public d'aujourd'hui sur la protection des infrastructures essentielles contre les attaques terroristes.

Les Pays-Bas s'associent à la déclaration qui a été faite tout à l'heure par l'observateur de l'Union européenne. Nous souscrivons également à la déclaration prononcée par S. E. M. Vincenzo Amendola, Sous-Secrétaire d'État italien aux affaires étrangères et à la coopération internationale, dans le cadre du partage de notre siège au Conseil de sécurité pour la période 2017-2018.

Je vais me concentrer sur notre stratégie nationale pour protéger nos propres infrastructures essentielles, ainsi que sur les enseignements tirés de notre expérience et sur le besoin de coopération internationale. Ma déclaration, dans sa version intégrale, sera disponible sur Twitter.

En ce qui concerne notre stratégie nationale, nous considérons qu'il est important d'avoir un cadre global permettant de déterminer les menaces qui posent un danger pour notre sécurité nationale, y compris nos infrastructures essentielles. Il convient de disposer d'un tel cadre global pour faire face à ces menaces. La protection des infrastructures essentielles fait partie de notre stratégie de sécurité nationale aux Pays-Bas et elle se fonde sur les réponses apportées à trois questions. Premièrement, quelles sont les menaces qui se posent à nous et quelle est leur gravité? Deuxièmement, que faisons-nous déjà pour y faire face et que pouvons-nous ou devons-nous faire de plus? Et troisièmement, comment mettre en œuvre les politiques qui s'imposent et renforcer nos capacités?

La réponse à cette dernière question est particulièrement déterminante et, bien entendu, relativement compliquée. Les éléments qui forment nos infrastructures essentielles appartiennent à 80% à des acteurs privés. Associer ces derniers n'est donc pas un choix mais une nécessité. Mais il y a de nombreux autres acteurs, notamment des organes mixtes, qui jouent un rôle important également. Dans notre stratégie, ces opérateurs essentiels, comme nous les appelons, sont les premiers responsables de la continuité et de la résilience des infrastructures essentielles dont ils sont propriétaires. Le gouvernement fournit pour sa part un cadre juridique et politique, et assure une fonction de supervision et d'inspection.

Nous avons tiré un certain nombre d'enseignements de notre expérience nationale spécifique. Aux Pays-Bas, nous appliquons une approche générale de la protection des infrastructures essentielles, qui englobe les menaces d'attaques terroristes. Quand on évalue les différents types de menace selon la même méthode, les risques deviennent comparables et il est donc plus facile de les hiérarchiser. Avec l'aide des secteurs public et privé, nous avons établi une liste complète des infrastructures essentielles, réparties en deux catégories, À et B. Les perturbations des processus de catégorie À ont des conséquences plus vastes que les perturbations des processus de catégorie B. Cette distinction nous permet d'allouer les ressources de manière plus efficace et rationnelle.

Nous nous appuyons également sur un système d'alerte antiterroriste. Lorsque nos services de renseignement détectent une menace terroriste grave à l'encontre d'un processus vital, les opérateurs et autres parties prenantes sont immédiatement informés. Des plans de sécurité renforcée définis à l'avance sont alors enclenchés afin de réduire la menace et de limiter les effets potentiels d'une attaque terroriste.

Cela m'amène à mon troisième point : le besoin de coopération internationale. Les efforts nationaux sont importants, mais l'action pour lutter contre les menaces terroristes pesant sur les infrastructures essentielles ne peut jamais être uniquement nationale. Certaines infrastructures essentielles, comme les aéroports, les systèmes énergétiques et Internet, sont internationales

par nature, et l'action pour contrer les menaces doit l'être tout autant.

Dans cet esprit, mon gouvernement a approuvé la semaine dernière la première cyberstratégie internationale de notre histoire. Elle définit dans quels domaines et comment coopérer avec les partenaires internationaux afin de garantir un cyberespace libre et ouvert, à l'abri des terroristes. Notre ministre des affaires étrangères, M. Koenders, a dit que c'est en coopérant avec d'autres pays au sein de coalitions que nous pourrons le mieux contrer les menaces qui se posent à nous. La résolution 2341 (2017), dont les Pays-Bas sont coauteurs, s'inscrit dans le même esprit. Je félicite l'Ukraine d'avoir facilité l'adoption unanime de la résolution aujourd'hui.

Comme cela est dit dans la résolution, la première étape importante vers une riposte internationale est d'échanger davantage les informations et les savoir-faire. Nous devons être inventifs et sortir des schémas de pensée habituels afin de réunir autour de la table les bonnes personnes. Les Pays-Bas coprésident actuellement le Forum mondial de lutte contre le terrorisme aux côtés du Maroc, et nous appuyons avec enthousiasme l'initiative en faveur de la protection des cibles non protégées lancée dans le cadre du Forum par les États-Unis et la Turquie. Cette initiative va au-delà des infrastructures essentielles et doit aboutir à un ensemble de pratiques optimales non contraignantes qui seront très utiles à l'ONU et à ses États Membres pour le travail futur sur la problématique qui nous occupe aujourd'hui.

Nous devons apprendre de nos expériences afin de prévenir autant que possible les attaques terroristes contre les infrastructures essentielles. Nous devons être bien préparés si hélas une attaque venait à se produire. Et surtout, nous devons le faire tous ensemble. Le terrorisme ne connaît pas de frontières, et notre coopération pour le combattre ne doit pas en connaître non plus. Nous devons être mieux préparés. Nous devons être mieux protégés. Nous devons avoir des partenariats plus forts. Nous devons mieux travailler ensemble.

Le Royaume des Pays-Bas est prêt à poursuivre sa coopération avec l'ONU et les États Membres pour protéger notre mode de vie contre les terroristes. Nous allons rester un partenaire du Conseil dans les efforts pour rendre le monde plus sûr.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant du Brésil.

M. Vieira (Brésil) (*parle en anglais*) : Je vous remercie, Monsieur le Président, d'avoir convoqué le débat public d'aujourd'hui. J'adresse mes remerciements à la Directrice de cabinet du Secrétaire général, Mme Maria Luiza Ribeiro Viotti, et à toutes les personnes qui ont présenté un exposé.

Le Brésil sait qu'aucun pays n'est à l'abri du terrorisme et il est donc très attentif à la prévention au niveau national mais aussi à l'échelle régionale et sous-régionale. Nous avons récemment mis à jour notre législation afin d'inclure sur la liste des infractions les préparatifs d'actes terroristes et le recrutement de combattants terroristes étrangers. Nous avons également simplifié les procédures de gel des avoirs des terroristes inscrits sur une liste par le Conseil. Nous avons réussi pendant la Coupe du monde de 2014 et lors des Jeux olympiques de l'an dernier, lorsque nous avons consolidé la coopération interinstitutions, tant au niveau national qu'au niveau international, à prévenir spécifiquement des actes de terrorisme ou l'entrée de terroristes présumés dans des lieux critiques comme les aéroports.

Les infrastructures essentielles sont en effet une cible privilégiée des organisations terroristes. La perturbation de la fourniture de services de base peut, après tout, avoir un effet déstabilisateur sur nos sociétés. Comme le souligne la note de cadrage (S/2017/104, annexe) établie pour ce débat, l'un des effets secondaires des progrès des technologies de l'information et des communications (TIC) est la plus grande vulnérabilité des infrastructures essentielles. L'établissement de normes qui permettent d'identifier et de proscrire l'utilisation abusive des TIC, et d'un cadre propice au renforcement de la coopération entre les États pour lutter contre cette utilisation abusive aiderait à mieux relever ce défi.

Le Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale a demandé à la communauté internationale de contribuer à améliorer la sécurité de l'infrastructure essentielle des TIC en développant des compétences techniques et en donnant des conseils sur la législation, les stratégies et la réglementation appropriées dans ce domaine. La nécessité d'aider au renforcement des capacités dans les pays les moins avancés fait partie intégrante de toute stratégie de lutte contre l'utilisation malveillante des TIC, et exigera des investissements plus importants et de longue haleine

dans les infrastructures et les services, le renforcement des capacités, la promotion de la recherche conjointe et la mise au point et le transfert de technologies. Les différences dans la capacité d'utiliser et de développer les TIC constituent un fossé des connaissances qui perpétue les inégalités, notamment entre pays développés et pays en développement, ce qui pourrait accroître les facteurs de vulnérabilité dans un monde interdépendant.

L'utilisation d'Internet et des réseaux sociaux par des groupes terroristes illustre la nature évolutive du défi auquel nous sommes confrontés. Ces plateformes sont également utilisées pour inciter à la haine, à des fins de recrutement et pour déclencher des attaques contre des infrastructures critiques. Alors que nous nous efforçons de lutter contre ces tendances, nous devons préserver la liberté d'expression et le droit à la vie privée. Dans ce contexte, nous soulignons l'initiative conjointe prise par le Brésil et l'Allemagne qui a donné lieu aux résolutions de l'Assemblée générale et du Conseil des droits de l'homme sur la question (résolution 68/167 et résolution 28/16, respectivement).

Des mesures répressives sont nécessaires mais ne suffisent pas pour éliminer le terrorisme. Le contrôle des frontières, la sécurité aérienne et maritime et l'application de la loi doivent s'accompagner d'efforts visant à remédier aux facteurs structurels qui favorisent le terrorisme, en particulier ceux associés à une marginalisation sociale, politique, économique et culturelle de longue date.

Nous devons agir contre les mesures qui ne respectent pas la diversité et ignorent notre humanité commune, telles que celles qui associent le terrorisme à des cultures, des religions ou à des groupes ethniques spécifiques. Il faut se garder d'une rhétorique qui alimente la xénophobie et les préjugés. Certaines réponses à la crise des réfugiés et aux mouvements migratoires récents sont également préoccupantes, car elles pourraient accroître plutôt que diminuer les risques associés à l'extrémisme violent pouvant conduire au terrorisme.

Il convient également de ne pas perdre de vue les conflits prolongés qui peuvent directement ou indirectement alimenter les programmes terroristes. L'incapacité à faire face aux crises en cours au Moyen-Orient, y compris le conflit israélo-palestinien, en est un bon exemple.

Les groupes terroristes cherchent à pousser les gouvernements à réagir de façon excessive, afin d'exploiter ces « exemples » de mauvais traitements et d'oppression. La lutte contre le terrorisme ne peut être efficace que dans la mesure où elle est compatible avec la Charte des Nations Unies et les autres normes du droit international, y compris le droit des droits de l'homme, le droit humanitaire et le droit des réfugiés.

Nous avons constaté une augmentation du nombre de lettres soumises au Conseil de sécurité au titre de l'Article 51 de la Charte, qui cherchent à justifier le recours à l'action militaire dans le contexte de la lutte contre le terrorisme, généralement a posteriori. Lors du dernier débat public sur les méthodes de travail (voir S/PV.7740), le Brésil a souligné la nécessité de donner suite à ces communications et de déterminer si les obligations énoncées dans la Charte sont remplies.

Rien ne saurait justifier les actes terroristes. Le Brésil réitère son engagement en faveur d'une réponse multidimensionnelle à cette menace et demeure convaincu que la coopération et le dialogue au sein de l'Organisation des Nations Unies renforceront notre capacité à atteindre les résultats nécessaires.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de l'Afghanistan.

M. Salarzai (Afghanistan) (*parle en anglais*) : L'Afghanistan remercie le Ministre des affaires étrangères de l'Ukraine, M. Pavlo Klimkin, et sa délégation d'avoir convoqué le débat d'aujourd'hui sur la protection des infrastructures essentielles contre les attaques terroristes. Nous sommes heureux de voir tant de pays participant au présent débat, preuve de l'importance du sujet à l'examen.

L'infrastructure est un élément clef du fonctionnement efficace et normal de la société, permettant l'accès des citoyens aux services fondamentaux, tels que l'approvisionnement en denrées alimentaires, en eau et en logements, la fourniture de soins de santé adéquats, des moyens de transport et des perspectives économiques, dont chacun est d'une importance cruciale pour la stabilité de tout environnement. Une attaque qui porte atteinte à l'infrastructure d'une nation est en substance un préjudice irréparable pour le tissu social même de la société. La protection de l'infrastructure physique et sociale doit donc être un élément clef de toute stratégie visant à garantir des sociétés pacifiques et stables.

Le terrorisme et l'extrémisme violent constituent des facteurs majeurs d'instabilité dans le paysage international actuel, causant des souffrances et des ravages indicibles aux populations et aux communautés.

Comme le montre clairement le cas de mon pays, l'Afghanistan, et de beaucoup d'autres pays où opèrent les terroristes, les forces extrémistes ont fait de grands efforts pour promouvoir leur programme maléfique – semant la destruction, sapant l'état de droit et terrorisant les populations. Elles ciblent ouvertement de nombreux types d'infrastructures afin d'amplifier les effets de leur barbarie et d'attirer l'attention des médias mondiaux.

L'Afghanistan est l'une des principales victimes du terrorisme mondial depuis plus de deux décennies – bien avant le début de l'engagement de la communauté internationale dans notre pays en 2001. Aujourd'hui, notre peuple reste fort face à une multitude de groupes terroristes tels que les Taliban, le Réseau Haqqani, Al-Qaida, Daech, Jamaat Dawa, Lashkar e Jhangvi, le Mouvement islamique d'Ouzbékistan et autres combattants terroristes étrangers, qui sont tous en symbiose les uns avec les autres, viennent de l'étranger et reçoivent, entre autres choses, une aide politique, idéologique, morale et matérielle. En plus de cibler nos forces de sécurité et celles des pays partenaires internationaux présents en Afghanistan, les extrémistes s'en prennent à nos institutions politiques et juridiques; aux mosquées et aux écoles; aux installations sanitaires et médicales; et à d'autres cibles vulnérables, telles que les organisations non gouvernementales qui s'emploient à améliorer la vie des Afghans ordinaires.

Pas plus tard que la semaine dernière, dans le cadre de leur carnage continu, un kamikaze a mené une attaque contre notre Cour suprême, la plus haute institution judiciaire du pays, tuant 21 personnes et en blessant près de 50 autres. Parmi les victimes figuraient plusieurs femmes juges, procureures et membres du personnel judiciaire qui rentraient simplement chez elles auprès de leur famille après une dure journée de travail.

Le mois dernier, le 11 janvier, les Taliban ont lancé une attaque contre le Parlement, faisant plus de 120 morts, et un nombre plus important encore de blessés et de mutilés graves. Cet acte de barbarie a été largement considéré comme une attaque contre l'infrastructure de notre démocratie, qui figure parmi les réalisations les plus importantes de l'Afghanistan depuis 2001.

En août de l'année dernière, des extrémistes ont attaqué l'American University à Kaboul, qui est vue comme une source d'espoir de vie meilleure par nos jeunes instruits et talentueux. De façon tragique, 16 personnes ont été tuées au cours de cette attaque.

En outre, il existe de nombreux cas d'hôpitaux locaux, de dispensaires et d'organismes internationaux de secours humanitaires qui sont attaqués ou subissent les répercussions néfastes des activités des groupes extrémistes. Il y a quelques jours, dans le nord de la province de Djozdjan, des militants de Daech ont tué six membres du personnel du Comité international de la Croix-Rouge (CICR), dans le nord de l'Afghanistan. Le convoi du CICR a été attaqué tandis qu'il acheminait de l'aide à une zone frappée par des orages.

Le climat général en matière de sécurité n'a fait que compliquer la situation humanitaire de notre population, au point que 9,3 millions de personnes, principalement des femmes et des enfants, ont cruellement besoin d'une aide humanitaire immédiate. Ce chiffre a considérablement augmenté depuis l'année dernière. Nous réitérons notre appel à la communauté internationale pour qu'elle appuie le Plan d'aide humanitaire de 2017 pour l'Afghanistan du Bureau de la coordination des affaires humanitaires.

Les terroristes posent également une menace aux projets d'infrastructures économiques et de développement, dans lesquels nous avons beaucoup investi. Nous travaillons actuellement pour mettre en œuvre 18 projets de coopération et d'investissement dans les domaines de l'énergie, des transports et des échanges, et dans les secteurs du commerce et de l'emploi. Une fois achevés, ces projets favoriseront la prospérité de l'Afghanistan et de l'ensemble de notre région.

Le cycle actuel de violence en Afghanistan n'est nullement un phénomène endogène. Ses causes profondes se trouvent ailleurs, en dehors de l'Afghanistan, et sont le résultat d'un plan stratégique élaboré au sein de notre région pour promouvoir un programme politique néfaste qui ne profite à personne, défie le droit international et constitue une violation flagrante de l'esprit même de la Charte des Nations Unies et des principes qui y sont consacrés, ainsi que des résolutions pertinentes de l'Assemblée générale et du Conseil de sécurité sur la lutte contre le terrorisme. Nous pensons que la lutte contre le terrorisme international est à la croisée des chemins. À cette étape critique, un meilleur effort mondial est nécessaire pour combattre cette menace avec davantage de précision et de justesse. Dans ce contexte, nous nous félicitons des efforts déployés par le Secrétaire général pour renforcer le dispositif de lutte contre le terrorisme de l'Organisation des Nations Unies, y compris sa décision de mettre en place un bureau de lutte contre le

terrorisme et de nommer un secrétaire général adjoint à la tête de ce bureau.

Malgré la difficulté de la situation en matière de sécurité en Afghanistan, nous sommes une nation qui avance à pas réguliers vers la stabilité durable et l’autonomie. Le Gouvernement d’unité nationale travaille dans une plus grande cohésion et une meilleure coordination pour relever un ensemble de défis complexes, auxquels est confrontée notre population. Dans le cadre de cet effort, nos forces de sécurité œuvrent avec courage pour améliorer la sécurité, tout en défendant et en protégeant notre souveraineté, nos infrastructures et notre population contre le terrorisme et l’extrémisme violent.

Pour conclure, nous considérons que la présente séance représente une avancée importante dans l’élaboration d’une démarche plus efficace de l’Organisation des Nations Unies pour la protection des infrastructures essentielles contre les attaques terroristes. En tant qu’organe principal de l’ONU chargé du maintien de la paix et de la sécurité, nous espérons que le Conseil de sécurité continuera d’accorder toute l’attention voulue à cette question importante.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant du Maroc.

M. Hilale (Maroc) : Qu’il me soit permis tout d’abord, Monsieur le Président, de vous féliciter pour l’accession de votre pays à la présidence du Conseil de sécurité pour le mois de février et pour la programmation de ce débat sur la protection des infrastructures contre les attaques terroristes. C’est une thématique fort importante, tant par sa pertinence que par son actualité.

Si l’homme a cherché depuis son existence à créer, à innover et à bâtir pour le bien-être de l’humanité et des générations futures, bien au contraire, les groupes terroristes, eux, ont choisi le chemin de la destruction, de l’anarchie et du néant. La menace terroriste ne cesse de s’accentuer et de se propager. Les groupes terroristes de Daech, d’Al-Qaida, des Taliban, de Boko Haram et autres, et leurs affiliés, renouvellent constamment leurs méthodes destructrices. Ils ne ratent aucune occasion de perpétrer des attaques contre les infrastructures sensibles, facilement accessibles, comme les aéroports, les stations de métro, les trains, les bus, les hôpitaux, les banques et les marchés, les écoles, les universités et les instituts. Les attaques perpétrées contre les aéroports de Bruxelles et d’Istanbul, ainsi que contre les stations de train de Londres et de Madrid, l’accès aux données des banques et des établissements étatiques, sont autant d’actes illustrant que les groupes terroristes sont prêts à attaquer n’importe quelle infrastructure et à exploiter la moindre faille de sécurité et de vigilance. Même les lieux de culte – mosquées, synagogues, églises – n’ont pas échappé à leurs actes macabres, alors que ce sont des lieux où les fidèles viennent chercher paix, quiétude et spiritualité. En outre, les installations nucléaires, chimiques, les dépôts de matériels radioactifs, les stations d’électricité, les barrages sont des sites très sensibles, exposés aux actes terroristes en l’absence de sécurité convenable. Ils sont susceptibles de devenir des bombes de destruction massive.

La menace terroriste sera accentuée davantage par le phénomène du retour des combattants terroristes étrangers dans leur foyer d’origine ou dans d’autres pays. Dans son dernier rapport sur la menace terroriste de l’État islamique d’Iraq et du Levant (Daech) (S/2017/97), élaboré en application de la résolution 2253 (2015), le Secrétaire général a mis en garde contre le phénomène du retour des combattants terroristes étrangers, après la défaite militaire de Daech dans plusieurs foyers. Le nombre de combattants terroristes étrangers en Iraq et en Syrie est estimé, selon ce rapport, à 40 000 combattants issus de plus de 100 pays. Ainsi le retour de ces combattants, bien entraînés aux techniques de guérilla et de confection d’explosifs, constitue une menace à la société et aux infrastructures sensibles. Ils peuvent agir individuellement, comme des loups solitaires, ce qui a amené le Secrétaire général à préciser que l’organisation terroriste dispose d’une grande capacité d’adaptation, en indiquant que la menace, à l’aviation civile également, demeure très élevée. C’est pourquoi la responsabilité de la protection des infrastructures sensibles incombe au premier chef à l’État, qui doit intégrer cette protection dans sa stratégie nationale de lutte contre le terrorisme et l’extrémisme violent. L’État doit s’assurer de la mise sur pied de moyens efficaces de protection et de sécurité, y compris par l’adoption des lois nécessaires à cet effet et leur renforcement, pour se conformer aux normes et exigences internationales.

Toutefois, le Maroc, qui a développé une approche globale et cohérente, orientée vers la prévention et l’action, considère que le terrorisme est un phénomène global qui nécessite et appelle une réponse globale, couplée et soutenue par une coopération très poussée à l’échelle sous-régionale, régionale et internationale. Le Maroc accorde une attention particulière à la coopération internationale, au renforcement de la sécurité des frontières, à l’échange et au partage des informations, à

l’utilisation de la base de données d’INTERPOL et à la mise sur pied des programmes de déradicalisation et de réinsertion pour faire échouer les plans des terroristes.

Le Maroc s’est engagé aux niveaux régional et sous-régional dans une coopération basée sur l’échange d’information, d’expertise et d’expérience, tant dans le cadre de la coopération Sud-Sud qu’avec des pays africains, qui, dans le cadre du bassin méditerranéen, y compris dans le cadre du groupe Cinq plus cinq, sont des partenaires régionaux. Le Maroc a accueilli des conférences en 2013 et 2015 sur la sécurité des frontières au Maghreb et au Sahel, et a participé en juillet 2015 à la réunion de Madrid. Il a pris part au Sommet sur la sécurité nucléaire, tenu à Washington, dont le communiqué final a appelé à plus d’efforts pour prévenir l’obtention par les acteurs non étatiques de matériaux nucléaires ou radioactifs à des fins de malveillance ou d’attaques contre des infrastructures sensibles.

Enfin, le Maroc, conscient de l’importance de la lutte contre le terrorisme nucléaire, participe activement à l’Initiative mondiale de lutte contre le terrorisme nucléaire depuis son lancement en 2006. Il a pris part à toutes les réunions et conférences organisées dans ce cadre et a organisé plusieurs réunions et ateliers de sensibilisation au profit de ses pairs africains. L’expérience marocaine dans ce domaine a été présentée la semaine dernière à New Delhi, en Inde, à l’occasion de la tenue de la réunion du Groupe de travail sur l’évaluation de l’Initiative mondiale de lutte contre le terrorisme nucléaire.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de la Pologne.

M. Winid (Pologne) (*parle en anglais*) : Je remercie le Président d’avoir organisé la présente séance et d’avoir inscrit la question de la protection des infrastructures essentielles contre les attaques terroristes à l’ordre du jour du Conseil de sécurité.

Nous nous associons à la déclaration prononcée tout à l’heure par l’observateur de l’Union européenne, mais je souhaite ajouter quelques observations à titre national. Si la Pologne a participé à la réunion organisée selon la formule Arria sur ce sujet par la délégation ukrainienne en novembre 2016, elle saisit aujourd’hui une nouvelle occasion importante d’aborder cette question des plus importantes.

Le terrorisme pose une menace croissante à la sécurité nationale et internationale. Il viole également les droits de l’homme, notamment le droit fondamental à la vie, et compromet le développement. Le Conseil de sécurité a souligné à maintes reprises que le terrorisme constitue une menace au maintien de la paix et de la sécurité internationales.

Les menaces ne respectent pas les frontières dans le monde globalisé contemporain. Les terroristes peuvent facilement infiltrer nos réseaux énergétiques et de transport les plus vulnérables. Il serait souhaitable d’élargir la portée géographique de la coopération. L’ONU est une enceinte appropriée, voire la meilleure, pour lancer le débat sur les mesures à prendre à cette fin.

La protection des infrastructures essentielles relève avant tout de la responsabilité des autorités nationales. La condition ultime pour assurer cette protection est l’efficacité des systèmes de sécurité nationale. Cependant, il est également possible de renforcer la coopération internationale. Cela est lié au fait que les menaces potentielles sont de nature transfrontières et qu’un grand nombre d’enseignements utiles peuvent être partagés entre les États. Dans ce contexte, la Pologne est disposée à partager ses expériences avec les pays partenaires et à appuyer les programmes visant à réformer le secteur de la sécurité.

Un bon exemple de coopération, dont la Pologne et l’Ukraine ont donné l’exemple, concerne la sécurité chimique, notamment les infrastructures chimiques essentielles. Des projets en la matière ont été mis au point, aux niveaux bilatéral et multilatéral, par l’Organisation pour la sécurité et la coopération en Europe (OSCE) et l’Union européenne (UE) et ont reçu l’appui du Partenariat mondial du Groupe des Sept : groupe de travail sur la sécurité chimique. La poursuite de ces efforts est de plus en plus importante, compte tenu du fait qu’un grand nombre d’installations chimiques sont situées en Ukraine, en particulier dans les zones de Donetsk et Louhansk, qui sont touchées par les hostilités et la guerre imposées à l’Ukraine de l’extérieur.

La Pologne et l’Ukraine ont également coopéré étroitement en 2012 lorsqu’elles ont coorganisé le Championnat d’Europe de l’Union des associations européennes de football. Cette collaboration a porté, entre autres choses, sur la protection des infrastructures de transport et sur les mesures de sécurité nécessaires à l’organisation d’événements sportifs de grande ampleur.

Je tiens également à souligner le rôle croissant des aspects internationaux de la protection des infrastructures essentielles. Les organisations

régionales, notamment l'OSCE et l'Union européenne, ont mis en place des programmes qui visent à structurer la coopération et l'échange d'informations. Par exemple, le cadre de l'OSCE englobe la sécurité des voyageurs et la protection des infrastructures énergétiques. La coopération au sein de l'UE porte notamment sur la création d'une base de données sur les voyageurs aériens, la coopération entre les gardes-frontière et les rapports de l'Office européen de police. Il a été recommandé d'élargir la coopération dans ce domaine pour couvrir une plus vaste zone géographique. Les liens entre les secteurs public et privé jouent également un rôle capital.

Enfin, j'accueille avec satisfaction la résolution 2341 (2017) sur la protection des infrastructures essentielles, qui a été initiée par l'Ukraine et adoptée ce matin et dont la Pologne s'est portée coauteur.

Je vous remercie une fois encore, Monsieur le Président, d'avoir organisé la présente séance.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant du Canada.

M. Bonser (Canada) (*parle en anglais*) : Le Canada est fier d'avoir parrainé la résolution 2341 (2017) adoptée aujourd'hui.

Les groupes terroristes évoluent et nous devons continuer à comprendre leurs stratégies afin de protéger nos populations. Par exemple, comme Daech subit des pertes en Iraq et en Syrie, il se transforme actuellement en califat virtuel mondial au lieu de l'entité associée à un territoire que nous avons connue. Les combattants terroristes étrangers encore loyaux à Daech qui ont été formés et qui possèdent l'expérience du combat constituent de nouveau une menace alors qu'ils vont ailleurs. La menace des terroristes agissant seuls et inspirés par des idéologies extrémistes violentes persiste. Comme les terroristes cherchent à provoquer le plus de dommages possible dans de nouveaux domaines d'activité, les infrastructures essentielles constituent une cible vulnérable.

Les attentats contre des actifs matériels, des systèmes de technologie de l'information, des réseaux et des services essentiels à la santé et à la sécurité peuvent être dévastateurs en ce qui concerne les pertes humaines, compromettre le bien-être économique collectif et éroder le sentiment de sécurité du public. Les attentats qui réussissent à faire beaucoup de mal et à causer des dommages importants appuient aussi les efforts de propagande des groupes terroristes. Les États Membres doivent travailler ensemble de manière concertée pour répondre à cet aspect de la menace terroriste mondiale dans le cadre de nos efforts collectifs. Par conséquent, nous accueillons favorablement la résolution présentée par l'Ukraine, qui encourage les États Membres à élaborer ou améliorer encore des stratégies visant à réduire les risques que présentent les attentats terroristes pour les infrastructures essentielles.

Dans notre contexte national, le Canada œuvre à tirer parti de ses réseaux du secteur des infrastructures essentielles pour mettre de l'information en commun et renforcer sa résilience contre les attentats terroristes. Une approche favorisant la collaboration des Gouvernements fédéral, provinciaux et territoriaux et du secteur des infrastructures essentielles a été établie dans le cadre de la stratégie nationale et du plan d'action canadiens sur les infrastructures essentielles, en vue d'atténuer l'éventail complet des risques et des menaces auxquels sont exposés les actifs et systèmes vitaux du Canada. La stratégie nationale vise à créer des partenariats, à mettre en œuvre une approche de gestion tous risques et à favoriser l'échange en temps opportun de l'information entre les partenaires et la protection de celle-ci. En dernière analyse, la protection de nos actifs et systèmes vitaux contre les menaces exige une approche concertée mettant en jeu un large éventail d'intervenants à tous les niveaux.

(*l'orateur poursuit en français*)

Nous soulignons la nécessité de cadres juridiques et réglementaires pour faire face à cette menace, et nous encourageons les organismes des Nations Unies à en tenir compte dans leurs évaluations des besoins en appui aux efforts de renforcement de la capacité des États Membres. Nous accueillons avec satisfaction cette résolution, qui renforce la protection des infrastructures essentielles dans le cadre d'une stratégie antiterroriste nationale et mondiale qui établit un équilibre entre les préoccupations de sécurité cruciales et les droits et libertés. Le Canada souscrit entièrement à la coopération au sein des États Membres et entre eux à tous les niveaux. Nous appuyons fermement cette résolution.

En terminant, nous profitons de l'occasion pour souligner l'engagement renforcé du Canada à l'égard de l'inclusion et de la diversité, à la suite d'un massacre ayant ciblé une mosquée de Québec, tuant six Canadiens. Comme l'a déclaré le Premier Ministre Trudeau,

> « Nous combattrons l'extrémisme sous toutes ses formes et nous serons là pour tous les citoyens et protégerons leurs libertés fondamentales,

la liberté de religion et de conscience, afin que toute personne puisse réaliser sa destinée en toute sécurité ».

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de la Malaisie.

M. Onn (Malaisie) (*parle en anglais*) : Je tiens à vous remercier, Monsieur le Président, d’avoir convoqué le présent débat public, et je m’associe aux orateurs précédents pour vous féliciter de l’accession de votre délégation à la présidence du Conseil de sécurité pour le présent mois. Je tiens également à remercier les intervenants de leurs exposés et de nous avoir fait part de leurs vues sur la question à l’examen.

La Malaisie est déterminée à lutter contre le terrorisme. Il est indéniable que les dommages causés aux infrastructures essentielles au maintien des fonctions sociétales fondamentales, que ce soit par des catastrophes naturelles, des actes de terrorisme, des activités criminelles ou des comportements malveillants, ont une incidence néfaste sur la sécurité d’un pays et le bien-être de ses citoyens. Il est donc important que les infrastructures nationales essentielles soient protégées contre les attaques terroristes.

Tous les gouvernements reconnaissent la menace que représente le terrorisme pour les infrastructures essentielles et les efforts soutenus de prévention et d’atténuation qu’exigent de telles menaces. Si la responsabilité de la protection des infrastructures essentielles contre les attaques terroristes incombe avant tout aux États, la mise en œuvre de mesures visant à réduire la vulnérabilité des actifs des particuliers et des actifs des entreprises relève en grande partie de la responsabilité des propriétaires de ces actifs.

Néanmoins, les sociétés privées ne bénéficient probablement pas d’incitations commerciales suffisantes pour financer des initiatives visant à réduire la vulnérabilité. Certaines entreprises peuvent estimer que les coûts afférents à la réduction des vulnérabilités dépassent les avantages découlant de la réduction des risques liés aux attaques terroristes et aux catastrophes naturelles ou autres.

Même si les gouvernements ont un rôle primordial à jouer dans la protection des infrastructures essentielles, le sens des responsabilités, la nécessité et la bonne gouvernance exigent des propriétaires de ces infrastructures essentielles qu’ils tiennent compte des besoins en matière de sécurité s’agissant de leurs biens. Par conséquent, les gouvernements et les entreprises doivent échanger des renseignements et des informations sur les menaces et les vulnérabilités et sur les mesures qui s’imposent pour protéger les infrastructures et réduire les risques.

À notre avis, le Groupe de travail sur la protection des infrastructures critiques, y compris Internet, les cibles vulnérables et la sécurité du tourisme a un rôle important à jouer dans les efforts déployés par la communauté internationale pour protéger les infrastructures essentielles des attaques terroristes. Ces efforts visent notamment la promotion de la coopération internationale et de la coopération entre les secteurs public et privé; le renforcement des capacités; le partage de meilleures pratiques; le renforcement de la réactivité et de la résilience grâce à la planification, à la prévention, à la gestion des crises et à des mesures de relèvement; la promotion de l’échange d’informations et de meilleures pratiques; et la mise en place d’un réseau d’experts en matière de protection des infrastructures essentielles.

Au niveau national, la Malaisie déploie des efforts en matière de protection des infrastructures essentielles à deux niveaux, au niveau fédéral et au niveau des États. Au niveau fédéral, ces efforts relèvent du Comité central chargé des infrastructures nationales essentielles, qui est dirigé par le Secrétaire général du Ministère de l’intérieur. Au niveau des États, le Comité des infrastructures essentielles est dirigé par le Secrétaire d’État. Dans le cadre de ces comités, des équipes d’audit ou de surveillance ont pour mission de surveiller le niveau de sécurité sur tous les sites d’infrastructures essentielles afin de détecter toutes les violations et de conseiller l’opérateur ou le propriétaire sur ce qu’il faut faire pour relever le niveau de sécurité sur les sites concernés. Pour ce qui est de la législation nationale relative à la protection des infrastructures essentielles contre les attentats terroristes, je pourrai citer la loi de 2016 relative au Conseil de sécurité nationale et la loi de 1959 portant sur les zones protégées et les lieux protégés. Nous nous sommes également dotés d’une politique nationale de sécurité cybernétique pour assurer la sécurité des infrastructures essentielles nationales d’information.

Le parrainage par la Malaisie de la résolution 2341 (2017), adoptée ce matin par le Conseil, témoigne de notre attachement aux efforts déployés par la communauté internationale dans ce domaine grâce au partage de meilleures pratiques, d’expériences, de compétences spécialisées et de renseignements en vue

de renforcer nos capacités pour sauvegarder et protéger les infrastructures essentielles des attaques terroristes.

Le Président (*parle en anglais*) : Je donne maintenant la parole à la représentante de l'Australie.

Mme Wilson (Australie) (*parle en anglais*) : La protection de nos infrastructures essentielles est un impératif économique et sécuritaire. L'Australie appuie l'initiative de l'Ukraine visant à mobiliser la coopération internationale pour prévenir les attaques terroristes contre les infrastructures essentielles et y réagir.

Le terrorisme fait peser sur les infrastructures essentielles des menaces persistantes, qui exigent des efforts soutenus de la part des gouvernements pour réduire les risques dans ce domaine. L'ONU a un rôle essentiel à jouer à cet égard, notamment en coopérant avec les États Membres en vue de la pleine mise en œuvre de la Stratégie antiterroriste mondiale des Nations Unies et des résolutions pertinentes du Conseil de sécurité.

Les pays définissent les infrastructures essentielles de diverses manières. Pour l'Australie, les infrastructures essentielles sont les installations physiques, les chaînes d'approvisionnement, les technologies de l'information et les réseaux de communication dont la destruction, la dégradation ou l'indisponibilité pendant une longue période aurait des effets graves sur le bien-être social ou économique du pays ou porterait atteinte à la capacité de l'Australie de garantir la défense nationale et d'assurer la sécurité nationale.

En janvier 2017, l'Australie a créé un centre d'infrastructures essentielles, qui propose une approche coordonnée et cohérente pour assurer la sécurité de nos infrastructures essentielles. Ce centre rassemble les compétences et les capacités nécessaires au sein du Gouvernement australien pour mieux gérer les risques liés à la sécurité nationale auxquels nos infrastructures essentielles sont exposées. L'Australie compte sur un solide système de prévention et de préparation en matière de renseignement à l'appui des mesures que nous avons prises pour lutter contre le terrorisme. Cette approche englobe des mesures ciblées de prévention et de préparation qui reposent sur des principes de gestion des risques et sur la disponibilité des capacités permettant de faire face à divers types de menaces terroristes et d'attaques terroristes, ainsi qu'à leurs conséquences. En outre, le Gouvernement australien travaille en collaboration avec les propriétaires et les opérateurs dans le cadre d'un partenariat entre entreprises et le Gouvernement pour mettre en commun les informations, tirer parti des expériences des uns et des autres et prendre des mesures d'atténuation concertées pour faire face aux risques les plus graves auxquels les infrastructures essentielles sont exposées.

Du point de vue des technologies de l'information, le centre australien de la cybersécurité est la principale entité qui fournit des conseils au Gouvernement australien en ce qui concerne les menaces cybernétiques. Nous sommes fermement convaincus qu'il est essentiel d'adopter une position robuste en matière de cybersécurité, de faire mieux connaître les vulnérabilités potentielles et de mettre en œuvre des mesures de sécurité efficaces dans le cadre des efforts déployés pour décourager et prévenir les incidents visant les infrastructures essentielles, notamment de la part des terroristes. La sûreté et la sécurité des infrastructures essentielles exigent des efforts concertés de la part des partenaires publics et privés dans le monde entier. L'Australie se réjouit à la perspective de continuer à coopérer concrètement avec des partenaires internationaux, y compris l'ONU, afin de renforcer et de promouvoir la sécurité et la résilience des infrastructures essentielles au niveau transfrontalier et mondial.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant de la Lettonie.

M. Mažeiks (Lettonie) (*parle en anglais*) : La Lettonie se félicite de l'initiative prise par l'Ukraine, durant sa présidence du Conseil de sécurité pour ce mois-ci, d'organiser ce débat important qui attire l'attention de la communauté internationale sur la question de la protection des infrastructures essentielles contre les attaques terroristes. Je remercie tous les intervenants de leurs exposés édifiants.

La Lettonie s'associe à la déclaration qui a été prononcée par l'observateur de l'Union européenne.

La propagation et l'intensité du terrorisme mondial sont, sans aucun doute, l'une des menaces les plus graves à la paix et à la sécurité internationales auxquelles nous sommes confrontés aujourd'hui. Durant l'année écoulée, rien qu'en Europe, nous avons été témoins de plusieurs actes terroristes ignobles, dont certains ont visé impitoyablement et délibérément des infrastructures essentielles. Les attentats qui ont pris pour cible l'aéroport et la station de métro de Bruxelles en mars dernier sont la preuve tragique que les terroristes ont semé la peur et continueront de répandre la peur et

le désarroi en perpétrant leurs attaques là où ils jugent qu’elles auront le plus d’impact.

Les attaques contre les systèmes de transport, les réseaux de télécommunications, les infrastructures énergétiques et les systèmes d’approvisionnement en eau peuvent souvent intensifier la perception de la menace terroriste, suite à un effet d’entraînement qui répand la peur parmi des populations qui ne sont pas touchées immédiatement par ces attaques. Par conséquent, la prévention de telles attaques grâce à l’introduction de mesures de protection adéquates pour les infrastructures essentielles revêt la plus haute importance.

La Lettonie s’est portée coauteur de la résolution 2341 (2017) sur la protection des infrastructures essentielles contre les attaques terroristes pour appuyer les efforts internationaux visant à renforcer la résilience face aux menaces terroristes.

En Lettonie, les mesures qui ont été prises pour protéger les infrastructures essentielles reflètent l’approche commune adoptée par l’Union européenne et se fondent sur les outils conçus par l’Union européenne à cette fin. Notre législation s’aligne étroitement sur les exigences énoncées dans la directive européenne sur les infrastructures essentielles européennes, contribuant ainsi à l’harmonisation des normes de désignation et de protection des infrastructures essentielles à l’échelle régionale, c’est-à-dire au niveau de l’Europe.

Nous avons créé une commission gouvernementale intersectorielle chargée de recenser et d’évaluer régulièrement les infrastructures essentielles existantes et potentielles afin de renforcer la sûreté et la sécurité de toutes les infrastructures qui auraient un caractère essentiel. Les exigences en matière de sécurité et de protection pour ces infrastructures sont très strictes, qu’il s’agisse de structures nationales, municipales ou privées. En outre, un point de contact a été désigné pour toutes les structures considérées comme étant des infrastructures essentielles nationales ou européennes en Lettonie, afin de faciliter l’échange d’informations avec les institutions nationales de sécurité. Pour renforcer les partenariats public-privé et renforcer les capacités en matière de sécurité et de protection des infrastructures essentielles, les institutions chargées de la sécurité intérieure organisent régulièrement des séminaires de formation et des ateliers sur le terrain pour les entités privées et publiques chargées de la surveillance et de la sécurité des infrastructures essentielles.

À l’heure de la mondialisation et dans ce monde où tout se tient de plus en plus, la numérisation et l’intégration des infrastructures essentielles grâce aux technologies de l’information et des communications font qu’il est encore plus nécessaire d’agir d’urgence pour assurer une protection globale et coordonnée au niveau international. À notre avis, c’est un domaine dans lequel l’ONU peut jouer un rôle clef en tant que cadre idéal pour l’échange de connaissances, de données d’expérience et de meilleures pratiques entre les États Membres.

Le Président (*parle en anglais*) : Je donne maintenant la parole au représentant des Maldives.

M. Sareer (Maldives) (*parle en anglais*) : Je voudrais tout d’abord féliciter l’Ukraine de son accession à la présidence du Conseil de sécurité pour ce mois et la remercier d’avoir organisé le débat public d’aujourd’hui sur la protection des infrastructures essentielles contre les attaques terroristes.

Au vu des exposés très instructifs présentés au Conseil de sécurité aujourd’hui, et compte tenu des contraintes de temps, je limiterai ma déclaration à quatre points clefs liés plus particulièrement à la nécessité d’adopter une approche intégrée et coordonnée en vue de protéger ces infrastructures contre les attaques terroristes.

Premièrement, il est essentiel que les efforts visant à améliorer la sécurité des infrastructures critiques contre la menace du terrorisme soient inscrits dans le cadre d’une stratégie nationale plus large et institutionnalisée de lutte contre le terrorisme et l’extrémisme violent. Cela est inévitable étant donné la nature complexe et interconnectée des menaces terroristes et des réseaux d’infrastructures modernes. L’action menée pour renforcer cette protection dépendra presque toujours de la fermeté des efforts faits dans d’autres domaines, coïncidant avec les objectifs d’autres initiatives visant à prévenir les actes de terrorisme. Le double emploi sape inutilement les efforts nationaux et gaspille des ressources financières, physiques et humaines généralement limitées.

Deuxièmement, le besoin de coordonner les efforts est particulièrement pressant pour les petits pays, notamment les petits États insulaires en développement (PEID) comme les Maldives. Conscient de ces faits, le Gouvernement maldivien a élaboré un cadre institutionnel robuste en vue d’adopter une approche coordonnée et englobant toute la société destinée à

contrer le terrorisme et l'extrémisme violent par le biais de mesures concrètes, ainsi que des politiques transversales. L'année dernière, nous avons mis en œuvre une politique nationale de lutte contre le terrorisme et l'extrémisme violent et sommes actuellement en passe de formuler une stratégie nationale antiterroriste, assortie d'un plan d'intervention antiterroriste dans le cadre de cette politique. La mise en œuvre de ces programmes sera guidée par le Centre national de lutte contre le terrorisme, qui a été créé l'année dernière et est chargé expressément de diriger et de coordonner le travail de toutes les institutions gouvernementales chargées de la lutte contre le terrorisme et l'extrémisme violent.

Un aspect clef de cette politique nationale est l'élaboration de programmes destinés à protéger les complexes touristiques et l'industrie du voyage, secteur crucial de notre économie, ainsi que des programmes de sécurité pour les ports, les aéroports et les infrastructures économiques majeures. Il s'agit là d'aspects fondamentaux de politiques visant à protéger les infrastructures critiques dans n'importe quel pays, mais leur importance n'est que plus amplifiée s'agissant des petits États insulaires en développement du fait de leur petite taille, de leur isolement géographique et de leurs ressources limitées. Une attaque terroriste contre les infrastructures essentielles serait dévastatrice, où qu'elle ait lieu. Mais tandis qu'une attaque, pour tragique qu'elle soit, n'aurait au final qu'un effet local dans un grand pays où de telles infrastructures existent en abondance, pour un petit pays insulaire qui dépend entièrement d'une seule infrastructure ou d'une poignée d'infrastructures, une telle attaque aurait un impact systémique. Pour les PEID, une attaque contre un aéroport international, un port maritime, une grande centrale électrique ou un réseau de distribution d'eau – des infrastructures qui n'existent qu'en « un seul exemplaire » – n'aurait pas seulement un coût humain mais priverait la population de ses moyens de subsistance et des nécessités matérielles et la couperait même du reste du monde.

Troisièmement, eu égard à l'importance amplifiée de la menace pour des pays comme les PEID faisant face à de considérables contraintes géographiques ou sociales, le renforcement des capacités et l'échange des pratiques optimales sont fondamentaux si tous les pays veulent pouvoir répondre efficacement à ces menaces. Les Maldives se targuent d'avoir bénéficié de la coopération de partenaires étrangers en matière de renforcement des capacités dans les secteurs de la sécurité, des soins de santé et des services publics, ce qui a permis à mon pays d'améliorer sa capacité de remédier et de répondre aux menaces qui se font jour contre les infrastructures critiques.

Quatrièmement, la nature transnationale et de plus en plus multisectorielle des organisations terroristes contemporaines, surtout celles liées à la criminalité transnationale organisée, exige que nous resserrions, aux niveaux bilatéral, sous-régional, régional et international, la coopération en matière de lutte contre le terrorisme et de protection des infrastructures critiques. Cela signifie également qu'il nous faut renforcer la capacité des organisations intergouvernementales – d'abord et avant tout l'Organisation des Nations Unies – d'aider à coordonner les stratégies antiterroristes.

À cet égard, nous devons nous engager de nouveau, tous ensemble, à apporter la dernière main à la convention générale sur le terrorisme international afin de pouvoir enfin traiter de ces questions dans le cadre d'un instrument juridique international détaillé et global. Il nous faut renforcer aussi bien notre participation nationale aux initiatives régionales visant à contrer la terreur et à prévenir l'extrémisme violent, que notre appui aux efforts multilatéraux des Nations Unies et d'autres organisations intergouvernementales, comme le Plan d'action du Secrétaire général pour prévenir l'extrémisme violent. À cet égard, nous prenons note des efforts faits par le Groupe de travail sur la protection des infrastructures critiques, y compris Internet, les cibles vulnérables et la sécurité du tourisme.

Tout comme les menaces posées par le terrorisme à tous les segments de nos sociétés, y compris les infrastructures critiques, continuent d'évoluer, les méthodes que nous utilisons pour les contrer doivent évoluer aussi. Cela ne doit pas cesser d'être un effort collectif, collaboratif et coordonné face au danger auquel nous faisons face. À cet égard, Monsieur le Président, vous pouvez compter sur l'appui sincère des Maldives.

Le Président : Je donne maintenant la parole au Représentant permanent d'Haïti.

M. Régis (Haïti) : Je tiens tout d'abord, au nom du Gouvernement de la République d'Haïti, à remercier 1e Gouvernement ukrainien de son aimable invitation à cette séance spéciale du Conseil de sécurité consacrée à ce thème d'importance majeure : la protection des infrastructures essentielles. Je salue la présence ce matin de S. E. le Ministre des affaires étrangères de l'Ukraine, M. Pavlo Klimkin, et prends plaisir à lui adresser mes

félicitations pour la qualité de son intervention et les pistes de réflexion et d'action qu'il nous a proposées.

Les Nations Unies ont fait de la mise en œuvre de la Stratégie antiterroriste mondiale une priorité essentielle. La protection des infrastructures cruciales en est incontestablement un axe majeur. Ma délégation souscrit pleinement aux objectifs de cette stratégie de riposte globale et intégrée, tant sur les plans national que régional et international.

La probabilité que soient commis des actes de terrorisme d'envergure prenant pour cibles des populations civiles en s'attaquant à des infrastructures essentielles n'a fait que croître ces dernières années. Le risque est partout présent, à des degrés divers, certes. L'émergence de nouvelles menaces, amplifiées par l'évolution rapide des technologies de la communication, accroît singulièrement cette probabilité, ainsi que la gravité de cette menace pour la paix et la sécurité mondiales.

Dans le combat sans merci qui doit être livré contre le terrorisme, Haïti est partie prenante du dispositif antiterroriste de l'ONU et de plusieurs mécanismes de coopération régionale mis en place au niveau de la Communauté des Caraïbes et de l'Organisation des États américains, notamment le Comité interaméricain contre 1e terrorisme. Au niveau national, le Gouvernement haïtien s'efforce de maintenir le niveau de vigilance adéquat à l'égard des menaces posées par des mouvements influencés par des idéologies extrémistes. Dans cette optique, il apporte son soutien le plus total aux efforts internationaux visant à renforcer la capacité des États à agir collectivement en matière de prévention de l'incitation au terrorisme et à améliorer la sécurité et la protection des cibles particulièrement vulnérables comme les infrastructures et les lieux publics, tel que le réclame expressément la Stratégie antiterroriste mondiale.

Cependant, force nous est de reconnaître que si les actes d'incitation au terrorisme sont fréquents, le dispositif international de lutte antiterroriste, en particulier pour ce qui est de la protection des infrastructures essentielles, demeure encore dramatiquement insuffisant. On en a pour preuve les menaces enregistrées, les tentatives avortées et les incidents dont nombre de pays en Europe, en Asie, en Afrique ou en Amérique ont fait les frais dans un passé récent. Car, si la montée en puissance du terrorisme semble avoir reçu ça et là un coup d'arrêt, son élan est loin d'avoir été brisé. Sa sphère d'action, si elle a été contenue sur certains théâtres d'opérations, est ailleurs en pleine expansion.

Il est donc primordial de redoubler d'efforts, d'intensifier la collaboration internationale sur tous les fronts, notamment en matière de coopération judiciaire et policière, d'échange d'informations, d'octroi d'une assistance technique appropriée et suffisante aux États qui en ont besoin, en particulier les moins avancés d'entre eux, afin de maintenir un haut niveau de protection des infrastructures cruciales, d'accroître la résilience contre les menaces terroristes et de prévenir les pertes de vies humaines et la perturbation des services essentiels, comme le souligne la note de cadrage du Ministère des affaires étrangères de l'Ukraine (S/2017/104, annexe). J'aimerais, à ce sujet, faire quelques brèves observations concernant la menace terroriste et la stratégie de riposte globale.

Tout d'abord, il apparaît primordial de bien cerner la menace terroriste afin de faire échec à ses actions que rien, par ailleurs, ne saurait justifier, ni les revendications nationales, politiques ou religieuses, généralement avancées par leurs auteurs. Le terrorisme ne peut être associé à une religion, une nationalité, une civilisation quelconque. Toutefois, il existe indéniablement un certain nombre de conditions propices à sa propagation, qu'il s'agisse de la persistance de conflits régionaux souvent à l'origine de l'extrémisme violent, de la discrimination, de l'exclusion, de la marginalisation socioéconomique, de la mauvaise gouvernance et de la pauvreté.

Par conséquent, il s'avère urgent pour la communauté internationale de s'attaquer à ces enjeux, de fournir aux pays en développement, notamment les plus démunis, l'aide adéquate dont ils ont besoin pour se doter des infrastructures indispensables et surmonter les graves défis auxquels ils sont confrontés sur le plan économique et social. Par ailleurs, ma délégation considère qu'aucun État, si puissant soit-il et quel que soit le degré de priorité qu'il accorde à la lutte antiterroriste, ne peut à lui seul atteindre l'objectif primordial de protéger ses citoyens et ses infrastructures essentielles. Les partenariats sont donc essentiels aux niveaux international, régional et national. Dans le même ordre d'idées, les mécanismes régionaux de lutte antiterroriste devraient être sensiblement renforcés et dotés de ressources adéquates leur permettant de mieux réagir en tenant compte des réalités et des besoins sur le terrain, ainsi que de l'évolution de la menace terroriste pesant sur les infrastructures cruciales.

Enfin, l'élaboration de réponses nationales intégrées pour la prévention du terrorisme et la protection des infrastructures essentielles revêt une importance particulière. Je voudrais, à cet égard, exprimer l'appui de ma délégation à la proposition ukrainienne d'incorporer un volet de protection des infrastructures cruciales dans tous les programmes nationaux et internationaux de prévention du terrorisme.

Pour sa part, le Gouvernement haïtien continuera d'accorder la plus haute attention aux mesures destinées à prévenir et combattre le terrorisme, y compris celles ayant trait à la protection des infrastructures essentielles. Des modifications ont été apportées récemment au Code pénal haïtien, renforçant ainsi la panoplie des mesures législatives et juridiques tendant à prévenir et contenir les idéologies de haine et l'extrémisme violent. La consolidation de l'état de droit, du système judiciaire, des organismes d'application de la loi est, à cet égard, l'un des axes d'intervention privilégiés du programme d'action défini par le Président de la République, M. Jovenel Moïse. Lors de son investiture le 7 février dernier, il a tenu à réitérer toute l'importance qu'il attache personnellement à la consolidation de l'état de droit en Haïti. Nul ne doute que le nouveau Gouvernement haïtien, qui prendra ses fonctions prochainement, sera fidèle à cet esprit et s'attachera à prendre les mesures qui s'imposent face à l'évolution de la menace terroriste contre les infrastructures cruciales.

La séance est levée à 15 h 45.